

**The Financial and Societal Costs of Institutional Data Breaches:
Evidence from Government and Hospital Breaches**

A Dissertation Presented for the
Doctor of Philosophy
Degree
The University of Tennessee, Knoxville

Banks N. Osborne

May 2025

Dedication

This dissertation is dedicated to all those who have walked alongside me during some of the most challenging, yet rewarding, years of my life.

I cannot begin this dedication with anyone other than my wife, Jackie Osborne. One paragraph will never fully encompass what you mean to me. You have always been a soothing soul when I need encouragement, a rock when I need stability, and a firework when I need energy. You knew what you signed up for over ten years ago, yet you still chose to sacrifice so much and endure more hardships because of my pursuit of this degree than anyone else will ever realize. Thank you for your consistent prayers and for believing in me when I did not. I consider this PhD just as much yours as it is mine.

Second, to my father, Richard Osborne, and my parents-in-law, Jim and Denise Merritt. Dad, I know that life has not always been easy for you. However, I hope that you know that your sacrifices have not gone unnoticed. Without you, I would not be the man that I am today. Jim and Denise, thank you for your incessant support and giving me a place to rest when I needed it.

Lastly, to some of my favorite professors. I am the product of your mentorship. Richard Dymmel, thank you for teaching me to always ask “Why?” Adam Jones, thank you for giving me a taste of research. Daniel Soques, thank you for instilling in me a love of research design and econometrics. And, of course, Ethan Watson, you have shaped me both personally and professionally in too many ways. It is because of you that I chose Finance and did not lose interest in research early in my academic career. I hope to inspire future students that way you did me.

I am grateful beyond words for all – named and unnamed – who have helped me get here.

Acknowledgments

I would first like to first express my gratitude to my dissertation chair, Matthew Serfling, for his continuous patience and for always providing the freedom needed to explore new angles and avenues of research. I could not have finished this dissertation without his years of support and flexibility.

I would also like to thank Zihan Ye for being a gentle mentor and introducing me to world of municipal finance. When I started my journey in Finance, I wanted to do research that is both interesting and relevant to the lives of normal, everyday people. During the third year of my program, I finally found such a niche that makes me excited to work.

Lastly, I want to show gratitude to Larry Fauver and Daniel Pienta for their insight, suggestions, and encouragement, and for being valuable members of my dissertation committee.

This dissertation benefits greatly from the invaluable comments given by seminar participants at Georgia Southern University, the University of Tennessee, the 2024 Financial Management Association, and the 2025 American Finance Association PhD student poster session.

Abstract

This dissertation examines how the effects of data breaches on governments and hospitals spill over to their stakeholders. The first chapter specifically considers the financial and societal costs of hacks on county governments. Using primary municipal bond market data, I find that hacks increase the cost of government debt and identify three mechanisms through which breaches influence investors' risk premium. Following a hack, county governments suffer lower credit ratings and decreased revenues. Hacked governments also cut social and infrastructure spending, which I argue increases their reputation risk and dampens their long-run economic competitiveness. Overall, these results in the first chapter suggest that data breaches harm municipalities both financially and socially.

In the second chapter, I exploit a unique aspect of HIPAA to examine how medical data breaches affect hospital financing costs and influence both hospital and patient health. As in the first chapter, I find that data breaches increase hospitals' cost of financing in primary municipal bond markets and increase hospitals' credit risk. However, investors seem to ignore hacks, the worst events, when pricing new bonds after a hospital announces a hack. This is surprising given that I find only hacks harm hospital cash flows and patient health. The mispricing of hacked bonds contrasts what would be expected given both theory and previous empirical evidence in the corporate finance literature. Furthermore, I find that cyber risk premium in municipal healthcare bonds exists only when investor attention is already heightened due to public awareness on cyber risk. Altogether, the results in my second chapter show that investors are not fully informed regarding how medical data breaches should influence local borrowing costs and, inadvertently, require higher premiums than necessary for some healthcare bonds and lower premiums than necessary for others.

Table of Contents

Chapter 1 – When Government Catches the (Cyber) Bug: The Costs and Real Effects of Municipal Cyberattacks	1
Abstract.....	2
1. Introduction.....	3
2. Data and Summary Statistics.....	12
3. Empirical Strategy and Results	18
3.1. Identification Strategy.....	18
3.4. Connection between Attacks and Other Risks	27
3.4.1. Credit Risk.....	27
3.4.2. Investor Beliefs Regarding Cash Flow Risk	28
3.2.5. Cash Flow Risk, Reputation Risk, and Real Effects of Attacks	30
4. Robustness Tests	36
4.1. Generalizability of Main Financing Tests	36
4.2. Alternative Counterfactuals.....	38
4.3. Alternative Approach to Dealing with Heterogeneous Treatment Effects	39
Chapter 2 – Data Breach Information, Hospital Financing, and Patient Outcomes.....	42
Abstract.....	43
1. Introduction.....	44
2. Institutional Details and Sample.....	51
2.1. HIPAA Notification Requirements	51
2.2. Bonds and Hospitals	54
2.3. Descriptive Statistics and Determinants of Breaches	56

3. Empirical Strategy and Results	58
<i>3.1. Identification Strategy.....</i>	<i>58</i>
<i>3.2. Impact of Breaches on Hospital Financing.....</i>	<i>61</i>
<i>3.3.1. Credit Risk</i>	<i>64</i>
<i>3.3.2. Hacks and the Role of Information Asymmetry</i>	<i>65</i>
<i>3.3.3. Hospital Health</i>	<i>66</i>
<i>3.3.4. Patient Health</i>	<i>68</i>
<i>3.4. The Role of Attention.....</i>	<i>71</i>
4. Robustness Tests	72
<i>4.1. Alternative Approach to Dealing with Heterogeneous Treatment Effects</i>	<i>72</i>
<i>4.2. Sample Construction and Alternative Counterfactuals.....</i>	<i>73</i>
5. Conclusion	74
References	76
Appendix.....	84
Vita	117

List of Tables

Table 1	96
Table 2	98
Table 3	99
Table 4	100
Table 5	101
Table 6	102
Table 7	103
Table 8	104
Table 9	105
Table 10	107
Table 11	109
Table 12	110
Table 13	111
Table 14	112
Table 15	113
Table 16	114
Table 17	115
Table 18	116

Chapter 1 – When Government Catches the (Cyber) Bug: The Costs and Real Effects of Municipal Cyberattacks

Abstract

I examine the costs and real effects of cyberattacks on U.S. counties using a stacked difference-in-differences research design. I find that data breaches increase the cost of municipal government debt, and I identify three mechanisms that link cyberattacks to increased costs. First, breaches increase a county's cash flow risk via significant decreases across several cash flow accounts. Additionally, breaches increase a county's credit risk and lead it to make budget cuts to social programs, which increases reputation risk. Overall, cyberattacks adversely affect municipal financing and influence counties to take actions that may lead to less-desirable future social and economic outcomes.

1. Introduction

“Local governments across the country are facing a growing threat of cyberattacks and escalating ransom demands, as an attack... has crippled thousands of computers for a month.”

- Scott Calvert & Jon Kamp, *The Wall Street Journal*, June 7, 2019

It is well-known that cyberattacks are costly to corporations. Unsurprisingly, cybersecurity experts predict that data breaches will cost the world over \$10 trillion in damages annually by 2025.¹ However, many such statistics focus only on the costs of corporate cyberattacks, and the extant cyber risk literature tends to focus solely on corporate outcomes after an attack (e.g., Kamiya et al., 2021; Crosignani et al., 2023; Florakis et al., 2023). Yet, corporations are not the only victims of cybercrime. Governments are popular targets for cybercriminals because of the lucrative data they keep and the potential to maximize an attack’s damage. The consequences for breached governments are unique in comparison to those of corporations, though, because attacks can impact more than just financial outcomes for the targeted entity. While governments face similar financial challenges as corporations, anecdotal evidence reports that targeted governments may have to reduce access to public services or make choices that impact their citizens’ lives both during and after an-attack (Calvert and Kamp, 2019a, 2019b). Despite the growing number of municipal attacks, little is known about how cyberattacks affect government financing or local outcomes.² In this paper, I address the broader consequences of data breaches by estimating the financial and real implications of cyberattacks for county governments.

¹ See “Cybercrime to Cost the World \$10.5 Trillion Annually by 2025”, *Cybercrime Magazine*, November 13, 2020.

² See “2022 Nationwide Cybersecurity Review”, Center for Internet Security, 2023.

Counties serve as a unique setting to study the broader implications of cyber risk. First, county governments have the potential to be attractive targets because of the data they hold and services they provide, such as keeping utilities operational, overseeing education systems, or trying to prevent crime. In contrast to corporations, though, county governments are especially vulnerable to cyberattacks because they have limited resources to devote to cybersecurity, aging computer systems, and difficulty recruiting cybersecurity talent (Calvert and Kamp, 2019a). Cyberattacks are potentially costly events that could prevent counties from collecting revenues or providing vital public services for weeks at a time (Calvert and Kamp, 2019b). The associated costs may even lead governments to redirect funding from public services to recover, potentially harming the potential long-run economic outcomes of their citizens and evincing an important quality of county cyberattacks not paralleled in the breaches of other entities. If cyberattacks lead to adverse financial outcomes or influence counties to make sub-optimal budget decisions, then investors should price any associated risks into the cost of municipal financing and targeted counties should have worse prospects than non-targeted ones.

My primary identification strategy exploits the staggered timing of cyberattacks on U.S. counties and identifies how the events directly influence county outcomes while controlling for county-specific factors. Because recent research suggests that staggered difference-in-differences specifications may suffer from biases arising from heterogeneous treatment effects over time, I employ a stacked difference-in-differences specification to overcome possible heterogeneity in my estimation of the average treatment effect on the treated over time (Baker et al., 2022). Additionally, I ensure my sample of data breaches avoids possible selection bias by including only hacks or involved malicious external actions in a data breach because targeted counties are obligated to report these breaches (Kamiya et al., 2021). Furthermore, I find that the propensity

for a county to be attacked is not strongly correlated with observable characteristics that may influence a hacker's decision to pursue it, such as its available cash or potential for technological security. Consequently, my identification strategy allows me to identify the impact of cyberattacks on county outcomes.

I begin my primary analysis by examining the relationship between cyberattacks and municipal financing costs. I find that targeted counties face higher costs for new issues. After a breach, targets suffer new offer yields that are 5 bps higher than what they paid pre-breach. In comparison to non-targeted counties within the same state, targeted counties face offer yields that are 11.5 basis points (bps) higher than non-targeted counties after an attack. Given the average issuance size of \$80.89 million, this implies that cyberattacks increase annual borrowing costs by about \$0.80 million for the average county, slightly larger than the impact of extreme weather events on municipal borrowing costs (Rizzi, 2023). A targeted county could fund the construction of a new elementary school with the increased interest it pays to investors over a 10-year period, which is the average bond's maturity in my sample (Cornaggia et al., 2018). Timing tests further indicate that targeted and non-targeted counties exhibit parallel trends before an attack, and the effect exists only after a breach. In fact, municipal borrowing costs increase as time progresses. The post-event disparity in borrowing costs between targeted and non-targeted counties is even greater for spreads over maturity-matched after-tax Treasury rates (approximately 25 bps) and is comparable to the increase in spreads caused by COVID-induced emigration (Gustafson et al., 2023). Furthermore, these results are robust to including county-level control variables. The results are also robust to alternative sample and econometric specifications, such as restricting the control group to neighboring counties, propensity score matching on county characteristics, expanding the sample of attacks to city governments and

bonds, and using Callaway and Sant'Anna's (2021) approach to correct for heterogeneous treatment effects over time. My results suggest the market prices cyber risk, and the cyber risk premium is great enough to lead county governments to potentially forgo valuable projects.

The municipal bond market also provides valuable insights into investors' expected cyber risk premiums for bonds of varying maturities. News and industry reports are often conflicted on whether the impact of attacks will be worse in the short-term or long-term. On one hand, anecdotal evidence suggests that most Internet-connected parties are not prepared for an immediate data breach, but on the other hand, cybersecurity experts expect the strength and consequences of attacks to outgrow cybersecurity defenses as time progresses (Brooks, 2022). As such, the municipal bond market may be divided in how they discount cyber risk for bonds with different maturities. If investors believe cyber risk will be greater in the short-, mid-, or long-term, then they will require a premium to invest in bonds of the corresponding maturity. Likewise, the associated premiums will reveal how investors believe cyberattacks will affect targeted municipalities over time.

Defining short-term bonds as those with maturities less than 3 years, long-term bonds as maturities greater than 10 years, and mid-term bonds with maturities between the other two, I find that investors require a premium for only long-term bonds from targeted counties. For example, investors require new offer yields that are 4.1 bps higher on targeted counties' long-term bonds post-breach. A similar situation is true when measuring the cost of financing with spreads over Treasuries (a 13 bps premium) and tax-adjusted spreads (an 18.1 bps premium). Investors do not require a premium that is statistically different from zero for any other subset of bonds. Additional tests show that the long-term cyber risk premium is statistically greater than the (insignificant) premium for short-term cyber risk premium. My results suggest that investors

believe the effects of cyberattacks will stick around after a breach, but the adverse effects will manifest only in the distant future. Investors view cyber risk as more of a threat to long-term cash flows.

Why might investors concentrate their expectations of cyber risk in a single subset of bonds given that the finance literature shows that many of the effects of cyberattacks tend to be concentrated in the years immediately following an attack (Kamiya et al., 2021; Tosun, 2021)? Given expert reports and anecdotal evidence on the state of cybersecurity, investors may be uncertain regarding the future of cybersecurity and how targets may respond to breaches. Additionally, investors may believe that targets will not fully realize the repercussions of an attack – either the financial or economic – until an indeterminant time in the future. Any immediate financial losses may not be as detrimental as any adverse longer-run economic changes. I address how cyberattacks affect the long-run economic consequences of targets in later tests.

Next, I seek to formally identify the connection between the municipal bond market's response to cyberattacks and counties' increased credit, cash flow, and reputation risk (e.g., Campbell et al., 2003; Tanimura and Wehrly, 2015; Amir et al., 2018; Akey et al., 2021; Kamiya et al., 2021; Ashraf, 2022). Regarding credit and cash flow risks, attacks may leave counties with large liabilities from lawsuits or other costs, affect their ability to collect revenues from projects, or encourage taxpayers to move to safer counties. Similarly, attacks are known to adversely affect corporate reputations, and targeted counties may choose to take unpopular measures, such as temporarily cutting funding to public services, to recover costs from attacks (e.g., Amir et al., 2018; Akey et al., 2021; Ashraf, 2022).³ Such actions may harm the public's trust in government

³ See “New Orleans Tech Chief Says City Continues to Recover after Cyberattack, though Coronavirus Has Brought New Challenges”, NoLa.com, June 16, 2020.

and potentially hamper long-run economic outcomes (Gundersen et al., 2011; Gao and Zhang, 2017; Vakili and Zhang, 2018; Jackson et al., 2021).

I first test the hypothesized credit risk channel by examining the ratings of targeted counties' bonds and issuing activity after an attack. I find strong evidence that rating agencies downgrade their ratings of targeted counties' new issues by about one-fifth of a letter grade. Given that average bond in my sample is on the lower end of an AA rating, an attack would downgrade a targeted county's future bonds to an AA- rating. However, despite targets' increased likelihood of default and the higher costs associated with new issuances, targeted counties do not disrupt their primary market issuance activity after a data breach. Attacks increase county credit risk, but counties choose to not drastically alter their financing patterns post-attack.

I next examine investor beliefs regarding municipal cash flow risk by comparing the premiums investors require for holding general obligation versus revenue bonds in sub-sample analyses. Revenue bonds are generally considered riskier investments because a county's ability to repay them is tied to a specific project's cashflow, but it is ex ante unclear theoretically which subset of bonds will be more affected by cyber risk because cyberattacks can affect funds from individual projects or those in general obligation (Cestau et al., 2019). Attacks could prevent governments from collecting revenues from specific projects or lead counties to use funds in general obligation to recover. In support of the former theory, I find that investors require a premium only for holding revenue bonds but there is no premium for investing in general obligation bonds. The cyber risk premium for revenue bonds ranges from 9.3 bps for new offer yields to almost 27 bps for tax-adjusted spreads. This finding supports the notion that investors believe that cyberattacks increase counties' cash flow risk, specifically through revenue

channels, and echoes fears in the popular press that attacks prevent municipalities from collecting funds for services for indefinite periods of time (Calvert and Kamp, 2019a, 2019b). However, this test is not enough to fully identify if attacks truly affect cash flows because the results show only where investors believe the effect is likely concentrated.

To further explore the cash flow and reputation risk channels, I use a stacked difference-in-differences design with an extended window to test two sets of longer-term county-level real outcomes. One set of variables measures various county-level cash flows, and the other measures county budgets for various social and public works programs. I utilize a window with a seven-year long post-period to better compare the long-term effect of attacks on county outcomes and long-run investor expectations. My methodology compares the post-breach outcomes of targeted counties to the targets' pre-breach outcomes, and my results are robust to controlling for both unique, time-invariant county factors that may influence a county's response to an attack and the general size of a county. I find that targeted counties' cash flows suffer across several dimensions after a cyberattack. The average target's general revenues and income from charged services decrease significantly in the period after a breach. Targets also deplete their insurance trust funds and sinking fund accounts at an economically meaningful rate. In response to losing revenues, targets also cut back their general expenditures, but their savings do not fully match their reduction in revenues. The data suggest that targeted counties face worse financial conditions than their counterfactuals for at least seven years following an attack.

I find further evidence that county governments cut their budgets for public services to offset the costs of an attack. For example, targeted counties decrease their police, public health, elementary education, natural resource, and public welfare budgets after an attack. Despite the traditional stability of county budgets, cyberattacks are associated with substantial budget cuts, a

trend reflected in anecdotal evidence from a non-trivial number of news reports. Such actions are more likely to increase a county's potential reputation risk, especially because budget cuts tend to be contemporaneously unpopular with constituents and stakeholders. Furthermore, reductions in social program spending may lead to adverse societal outcomes and indirectly affect a county's future economic or financial wellbeing (Gundersen et al., 2011; Gao and Zhang, 2017; Vakili and Zhang, 2018; Jackson et al., 2021). My results suggest that cyberattacks lead counties to take actions that harm their own reputation and could increase investor uncertainty regarding future economic outcomes, helping to explain why investors' cyber risk premium is concentrated in long-term bonds (Grigoris, 2020).

My paper differs from the contemporaneous working papers of Andreadis et al. (2023), Curti et al. (2023), and Jensen and Paine (2023) in a couple of important dimensions, although all of our studies focus on county-level responses to cyberattacks. First, our samples differ. Jensen and Paine (2023) employ only ransomware events. Andreadis et al. (2023) aggregate all the attacks (including on firms) that occur within a county to the county-level and implicitly assume that the number of non-government breaches will affect municipal financing. In contrast, I consider only government-related attacks when identifying the effect of cyberattacks on county financing. Second, our primary research questions and hypothesized channels differ. Andreadis et al. (2023) identify the role that local newspapers play in disseminating information about data breaches and propose information-based links between cyberattacks and yields. Curti et al. (2023) suggest that increases in government operating costs are the reason borrowing costs increase. Jensen and Paine (2023) do not look at municipal borrowing costs but, instead, focus on the relation between cyberattacks and optimal investment in information technology by the government. Instead, my paper introduces three new mechanisms that relate attacks to

government financing costs. Not only do I show that cyberattacks increase counties' credit and cash flow risks, I also connect cyberattacks to a county's reputation risk and show how breaches could affect broader non-financial, societal outcomes. Relatedly, no other paper considers the social implications of cyberattacks. Although Andreadis et al. (2023) and Curti et al. (2023) study how attacks affect county-level investment, neither paper estimates how counties alter their spending towards specific social programs. In contrast, my study quantifies the direct effect of attacks on several different programs.

My paper makes several contributions to the literature. First, to the best of my knowledge, my paper is among the first to use the municipal bond market as a setting to identify the financial costs of attacks for governments and to examine the economic costs of cyberattacks. My results speak to the larger societal costs of data breaches by quantifying increased interest expenses for targeted counties and showing how targeted counties reallocate funding from public services to recover from attacks. As such, there are regulatory and governance implications from my research. My results imply local governments may want to consider alternative sources of funding (i.e., cyberattack insurance policies with larger coverages) to recover from data breaches. Governments, likewise, may benefit from incorporating stronger data protection policies or hiring more cybersecurity experts. Additionally, targeted governments may benefit from establishing programs that help convince citizens that their choices to temporarily reallocate funds from public services will ultimately be value enhancing.

Second, my research adds to a growing literature on cyber risk. The extant literature has focused primarily on corporate outcomes. Much of the early work identifies how attacks influence targets' short-term market value (e.g., Campbell et al., 2003; Hovav and D'Arcy, 2003; Cavusoglu, Mishra, and Raghunathan, 2004; Amir, Levi, and Levine, 2018). More recent

literature has begun to examine other potential effects of attacks and breaches for publicly traded firms (e.g. Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Tosun, 2021; Crosignani et al., 2023). I extend this branch of the literature by showing that cyber risk is not limited to just public firms and that attacks have both economic and financial consequences for municipalities.

Lastly, my results contribute to an established literature on risk factors in municipal bonds. Examples of recently discussed factors include political corruption (Butler et al., 2009), newspaper closures (Gao et al., 2020), climate change (Painter, 2022), opioid use (Cornaggia et al., 2022), COVID-induced emigration (Gustafson et al., 2023), and climate-related events (Jerch et al., 2023; Rizzi, 2023). My paper shows that investors price cyber risk in the municipal bond market and identifies potential channels that explain why investors account for cyber risk.

The rest of my paper proceeds as follows. Section 2 describes my data, and Section 3 outlines my identification strategy and results. Section 4 provides robustness tests. Section 5 concludes and highlights policy recommendations for government data security.

2. Data and Summary Statistics

I use multiple data sources in my analysis. Using cyberattack data from the Privacy Rights Clearinghouse (PRC), I begin by identifying counties that were hacked and involved malicious external actions in a data breach to avoid potential sample selection issues associated with events that are not necessarily mandatory reporting events (Kamiya et al., 2021). I further restrict my sample of attacks to those on counties that issued municipal bonds. These restrictions yield a total of 17 attacks on 15 unique counties in 12 states from 2005 to 2016, and Appendix A lists these events.⁴ I assign a variable *Target* that equals one to each of the targeted counties and

⁴ The PRC database identifies 148 hacks, not including other types of internal data breaches, on government entities over my sample period, but the majority are at the federal level. There are only 9 hacks on states and 23 on cities.

zero for all other non-targeted (i.e., control) counties in the same states. Although the number of cyberattack events is small, the events correspond to a large number of treated bonds and parallels studies that use changes in state-level laws (i.e., wrongful discharge laws) that affect a large number of corporations in a small number of states (Serfling, 2016).

I include only attacks on counties rather than attacks on other political units in my primary sample for three reasons. First, focusing on only counties for my primary analysis helps me keep a consistent research design throughout my whole study, which ultimately addresses how cyberattacks affect real county-level outcomes. Second, I can easily quantify the longer-term consequences of cyberattacks for counties because the Census Bureau makes annual county-level data readily available. Lastly, counties tend to serve more as administrative units as they focus on providing public services rather than legislation and are much less likely than other political levels to pass laws or institute new regulations pertaining to cyber risk that coincide with a data breach's timing. This final reason allows me to more cleanly employ a difference-in-differences-type methodology without confounding the effect of cyberattacks with the impact of a contemporaneously passed law or resolution that may influence investors' expectations of cyber risk.⁵ These differences between counties and other levels of government are important in determining if cyberattacks affect more than just government financing costs, a key distinction of

My search initially finds 20 hacks on counties, but three counties (Sierra County, CA; Glades County, FL; and Lincoln County, ME) do not issue bonds. As such, I drop these three events and the associated counties from my sample for my bond-level and county-level channel tests. I later test for robustness towards the inclusion of city bonds, but I do not consider state bonds in order to keep a consistent research design that cleanly focuses on county-level outcomes.

⁵ See "How County Governments Work", FindLaw.com, June 30, 2021. Although county governments do pass laws and have their own ordinances, it is much more common for U.S. counties to not have much authority over their own legislative capabilities. Furthermore, although counties are not immune to state laws, I assume that a state is less likely to pass a law regarding cyber risk in response to a county-level attack than it would be if a state-level entity were attacked.

my study. Nonetheless, I address the generalizability of my results to all levels of local financing by expanding my sample of attacks to those on city governments and city bonds in Section 4.

I consider a hack to be an attack on a county if the PRC database specifically identifies the target as a U.S. county or a government-related, county-level administrative unit.⁶ I implicitly assume that a data breach that involves any branch of a county's government, whether a sheriff's department or park management system, is an attack on the entire county for two reasons. First, county governments are unlikely to have many cybersecurity teams dedicated to specific entities.⁷ If a county has retained any cybersecurity talent, the experts' attention would likely be stretched thin across several entities under the county's oversight, especially during and after an attack. Second, the PRC database does not always specify the exact department that hackers breached. Although I can sometimes identify the exact government entity that hackers targeted (i.e., the Sheriff's Department of Berrien County, Michigan), PRC does not record specific departmental targets for a little under half of my sample of attacks. These restrictions further imply that I do not assume that an attack on a city or other entities within a county is an attack on the county itself, differentiating my sample of events from that of Andreadis et al. (2023). My sample restrictions further separate my primary sample from that of Curti et al. (2023), which includes attacks on cities and states, and of Jensen and Paine (2023), which includes only ransomware events.

⁶ The PRC database identifies all government targets with the *Type of Organization* flag "GOV". I search the PRC's records of county target names for the strings "county" to ensure I do not include data on cities that have the same name as their respective county (e.g., Los Angeles County vs Los Angeles, CA). I also search for the term "district" to capture possible scenarios when attacks target county-level services whose presiding counties are not directly named (e.g., Foothills Park and Recreation District). In the latter case, I manually record the associated county and state. I manually validate each event in my sample.

⁷ See "Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It", Governing.com, May 6, 2022. Also see the New York State Association of Counties whitepaper "Cybersecurity Primer for County Leaders", September 2022 for an excellent overview of the current state of county governments' cybersecurity talent. Further note that this differs from the experience of state-level entities that are more likely to have greater access to cybersecurity task forces: see "Cybersecurity for the States: Lessons from Across America, NewAmerica.com.

I collect data on municipal bonds from SDC Platinum’s Global Public Finance database for U.S. bonds. Specifically, I identify county-level bonds by restricting my sample to bonds whose issuers are listed as counties, parishes, local authorities, or districts and match the issuers to target and control counties by name and state. In addition to *Yield*, I additionally proxy for the risk premiums investors demand for investing in municipal bonds with yield spreads using two definitions (Cornaggia et al., 2022; Tran and Uzmanoglu, 2022). I first compute *Spread* as the difference between municipal bond yields and maturity-matched Treasury bond yields, using linear interpolation of Treasury yields when an exact match is unavailable. Alternatively, I compute *Adjusted Spread* as the after-tax spread over Treasuries by using the highest marginal tax rates.⁸ For my main analysis, I keep all rated bonds issued within a seven-year window around an attack (i.e., three years before and three years after).

Lastly, I collect county-level economic data from two sources. County characteristics, such as population, employment, and per capita income come from the Bureau of Economic Analysis. Real and financial county data ultimately come from the Census Bureau, but I use a cleaned, named dataset provided by Pierson et al. (2015) to facilitate my research. I match the economic data to bond issuers on county and state names and year but use lagged county characteristics in my analysis to avoid possibly endogenous control variables.

Table 1 presents summary statistics for the main variables in this study in Panel A and compares targeted and non-targeted observations in Panel B. Panel C presents an overview of the county-level financial accounts I examine in my study. Appendix B describes variable definitions. All continuous variables are winsorized at the 1st and 99th percentiles. My total sample includes 444,368 municipal bonds and 11,596 county-years. The average bond in my

⁸ State tax rates come from <https://www.taxpolicycenter.org/statistics/historical-highest-marginal-income-tax-rates>.

sample has an initial yield of 3.1%, matures a little past 10 years after issuance, and provides a county \$2.2 million in funding. However, the average (median) total issue size is \$80.89 million. About 57% of bonds are funded via counties' general obligations, and 43% are funded via project revenues. Although there are about 59k treatment observations and 426k control observations, there appear to be few major differences between my treated and control subsamples. Targeted (control) bonds have an average initial offer yield of 2.97% (3.11%), spread over Treasuries of 1.10% (1.16%), *Adjusted Spread* of 2.46% (2.51%), and maturity of 10.2 years (10.2 years). The bonds across both groups have similar average ratings. Ninety-one percent of both targeted and non-targeted bonds are callable, and a little over half of both subsamples are general obligation bonds. Targeted and non-targeted counties' per capita incomes in the year prior to the data breaches are also similar. However, the average non-targeted bond issuance is a little larger than the average targeted bond. Likewise, targeted counties are larger than control counties. These similarities, and differences, prompt me to examine if county cyberattacks are correlated with any observable covariates.

I preface my primary analysis by examining the determinants of municipal attacks in **Table 2**. I use a linear probability model to estimate the likelihood that a county is targeted in any given year by conditioning on several factors. The independent variables I include are meant to capture observable characteristics that may influence a hacker's decision to pursue a county. For example, the variables *Total Revenue*, *Total Income Tax*, and *Total Cash* all measure a county's potentially available (i.e., stealable) funds or ability to pay hackers' ransoms. The variables *Population*, *Per Capita Income*, and *Employment* capture the possible breadth and desirability of residents' data and the level of county wealth. The binary variable *Urban*, defined by the National Center for Health Statistics's 2013 Urban-Rural Classification Scheme, helps to

identify if urban counties are more likely to be targeted than rural counties, possibly because the former are more visible or accessible to hackers (or if rural counties have weaker defenses due to lesser technology). I use lagged, logged-transformed independent variables in Models 1-3 and the first difference of logged-transformed data in Models 4-6. Models 1 and 4 include state-year fixed effects to control for unobserved factors that influence the propensity of a county's attack within a state-year, such as local economic conditions; unobserved, time-varying state-level characteristics; and potential "cyberattack waves" described in Kamiya et al (2021). Models 2 and 5 add county fixed effects to account for unobserved county-level factors, such as a county's degree of technological advancement, that may influence the outcome of successful cyberattacks. Models 3 and 6 drop the state-year fixed effects and add year fixed effects to more closely align with my preferred specification discussed in the following section. I estimate the variable *Urban* only in Model 1 because it is either collinear with county fixed effects or has no variation in a first difference model.

I find that no one factor is a consistently strong predictor of municipal cyberattacks, including the finance-related variables. This potentially suggests that hackers do not target counties for direct financial gain via the theft or ransom of government funds. Instead, a county's population and per capita income weakly predict its propensity to be attacked. Larger and wealthier counties may be slightly more likely targets for attacks, but these relationships are inconsistent across the models. Nonetheless, I choose to follow the municipal bond literature and control for *Population*, *Per Capita Income*, and *Employment* in my later analyses to account for any possible effect these characteristics may have on municipal bond investors' responses to an attack (Cornaggia et al., 2018; Gustafson et al., 2023).

3. Empirical Strategy and Results

In this section, I examine how cyberattacks affect county financing costs and identify the channels through which data breaches influence investors. I also document the real effects of attacks through this process.

3.1. Identification Strategy

My primary model is the following stacked difference-in-differences regression specification with three years of pre-attack and three years of post-attack data (i.e., a seven-year window):

$$y_{i,t} = \beta_1 Target_i \times Post_t + \beta_2 Target_i + \beta_3 Post_t + \gamma' Controls_{i,t} + \omega_{s,e} + \varphi_{t,e} + \varepsilon_{i,t}. \quad (1)$$

My primary dependent variables include *Yield*, *Spread*, and *Adjusted Spread* for the municipal financing models. The coefficient β_1 estimates the impact of cyberattacks on county outcomes and is my coefficient of interest. *Target* is an indicator that equals one if a bond is issued by a county targeted by an attack and zero otherwise. *Post* is an indicator that equals one if a bond is issued after a county suffers a data breach. Following the municipal bond literature, I include several bond and county characteristics as controls. The continuous bond characteristics I include are a bond's coupon rate, maturity, inverse maturity, and corresponding maturity-matched Treasury yield (which I exclude from the *Spread* and *Adjusted Spread* models). I also control for whether an observation is a callable, negotiated, insured, tax exempt, or general obligation bond with respective indicator variables. Following the municipal bond literature, I include the issuing county's prior year's population, per capita income, and employment to account for any potential differences between target and non-target counties and to control for factors that may affect a county's ability to repay its debts (Cornaggia et al., 2018; Gustafson et al., 2023). Although my results hold with the inclusion of a bond's max rating at issuance as a control variable, I do not

include it in my primary analysis because it is an endogenous control variable, as I hypothesize that credit risk is one of the channels through which cyberattacks influence county finances. As is additionally common in the literature, I drop any bonds with negative *Spread* or *Adjusted Spread* from the respective analyses, though my results are robust to their inclusion in the sample (Gustafson et al., 2023).

I use a stacked difference-in-differences specification because standard staggered difference-in-differences models may possibly be subject to biases arising from heterogeneous treatment effects over time. In fact, estimates of the average treatment effect on the treated (ATT) produced via staggered difference-in-differences estimators may even have the opposite sign of the true treatment effect. I overcome this challenge by implementing the stacked difference-in-differences estimator (Cengiz et al., 2019). Following Baker et al. (2022) I structure my data in such a way to create an attack-specific dataset for each treatment group and its clean control group to represent a singular “experiment” for each event. Treated counties are those that are targeted by a cyberattack, and treated bonds are any bonds issued by a targeted county. Control counties are those that are never targeted but are in the same state as the target. For example, one “dataset” includes all bonds for Franklin County, Ohio, and bonds for all other non-targeted counties in Ohio. Next, I “stack” all the attack-specific datasets together. Even though each attack happens at a different time, the stacked dataset aligns all the attack-specific datasets together in event-time because I take a sample of bonds within a seven-year window of each attack. As such, I essentially have seventeen quasi-natural experiments from which to estimate the impact of cyberattacks on municipal financing costs.⁹

⁹ The events are the announcement dates of the breaches outlined in Table A of the Appendix.

Alongside the stacked difference-in-differences design, I include county-event ($\omega_{s,e}$) and year-event ($\varphi_{t,e}$) fixed effects in my primary model to further ensure my comparisons of treatment and control outcomes are within the same county, year, and experiment. I choose to cluster standard errors at the county-level to account for residuals being correlated within a county over time.

My identification exploits variation from multiple sources. First, it relies upon the clean separation of treatment and control groups. Further, I force all comparisons of treated and control outcomes to be within the same county and year to difference out any unobserved cross-sectional and time series factors that might affect both treatment and control groups simultaneously (Cornaggia et al., 2022). This first difference helps ensure that my estimate of the average treatment effect on the treated, β_1 , is not biased by any omitted variables – such as a county’s own political economy or other macroeconomic conditions – that might be relevant to either group’s outcomes post-attack.

Second, my identification strategy exploits the staggered nature of cyberattacks. Attacks randomly target certain counties between 2005 and 2016, allowing me to capture all relevant events over the sample period and mitigate concerns that a contemporaneous trend might confound the treatment. Treatment counties enter my sample three years before they suffer a data breach and exit three years afterwards, so I observe both their pre- and post-attack financing costs. I assign the breach date of the targeted county to all non-targeted counties in the same state because control counties do not experience their own data breach and observe their pre- and post-attack outcomes over the same seven-year window centered on the target’s breach. My model differences out any unobserved time-invariant state-specific factors, such as the effect of a state’s culture and attitude towards technology, that may endogenously affect a county’s

financing. As such, this difference-in-differences forms a quasi-natural experiment that allows me to identify the effect cyberattacks have on targeted counties' cost of capital.

3.2. *Impact of Attacks on Municipal Financing*

I begin by quantifying how cyberattacks impact county financing costs using the dependent variables *Yield*, *Spread*, and *Adjusted Spread* in **Table 3**. Inspired by recent municipal bond research that utilize state fixed effects, I first utilize state-event fixed effects in Models 1, 3, and 5 to compare the effect of cyberattacks on county financing to other factors that influence the cost of government debt. Somewhat unsurprisingly, targets have lower financing costs pre-attack, though the difference is not statistically significant. Despite the lower pre-breach costs, each model shows that targeted counties suffer increased financing costs after a cyberattack. Model 1 shows that targeted counties' initial offer yields are 11.5 bps higher relative to bonds issued by non-targeted counties in the same state and year after an attack. Economically, this translates to a 3.7% increase in annual borrowing costs – about \$0.80 million for the average county – and is greater than the impact of extreme weather events on municipal borrowing costs detailed in Rizzi (2023).¹⁰ A targeted county could fund the construction of a new elementary school with the increased interest it pays to investors over the life of the average bond in my sample (10 years) (Cornaggia et al., 2018). Similarly, Model 3 shows that targeted counties drastically increase their spreads over Treasury rates around 19.0 bps, comparable to the increase in spreads caused by COVID-induced emigration (Gustafson et al., 2023). Model 5 shows the targeted counties' post-attack increase in *Adjusted Spread*, 25.3 bps, represents an 11.0% increase over the sample mean of *Adjusted Spread*.

¹⁰ I utilize the modified duration approach to calculate the increase in borrowing costs for targeted counties. \$0.80 M = \$80.09 M (mean annual issuance) $\times$ 8.6 (mean duration) $\times$ (0.00115/(1 + 0.0309/2)).

However, the specification with state-event fixed effects could be biased because it does not fully follow the stacked difference-in-differences estimator with unit fixed effects presented in Baker et al. (2022). To address this concern, I replace the state-event fixed effects with county-event fixed effects to capture variation within a county's own financing costs surrounding an attack. This alternative specification differences out any time-invariant, county-specific attributes, such as a county's political leaning or level of financial literacy, that may influence responses to data breaches. I present the results with the county-event fixed effects in Models 2, 4, and 6 of **Table 3**. The magnitudes for both spread-based outcomes with county-event fixed effects are economically similar to those estimated with state-event effects. I find that targeted county spreads and tax-adjusted spreads increase 12.6 bps and 17.8 bps, respectively, post-attack. The cyberattack premium still exists in new offer yields, as well, after accounting for time-invariant county-level effects. My results are robust to the inclusion of unit fixed effects, and I choose to use county-event fixed effects for the remainder of my primary analysis as it is more stringent than the state-event fixed effects.

My identification strategy and interpretation of the stacked difference-in-differences estimator relies on the parallel trends and exogeneity assumptions of any standard difference-in-differences test. I first test the parallel trends assumption for each of my dependent variables with a dynamic analysis in **Figure 1**. Specifically, I replace *Post* in Eqn. (1) with six indicator variables to capture the subperiods surrounding the year of attack and, following econometric tradition, use the year immediately before the event as the reference period. I plot the timing coefficients based on models with and without control variables. Given that all of the coefficients for the pre-periods are statistically indifferent from zero, I find no evidence that the treatment and control bonds follow different trends before a county is targeted. Instead, I find evidence that

municipal borrowing costs increase as time progresses after an event, and the effect seems to persist for at least three years following a breach. It is important to note that the post-trends are significant only when estimated in the model with control variables, suggesting that the bond- and county-level control variables are necessary to precisely estimate the unit-level treatment effect.

Likewise, endogeneity is unlikely to be a major concern. First, attacks are always unexpected shocks and, many times, undefendable events for even the largest, best-equipped corporations (Kamiya et al., 2021; Crosignani et al., 2023). It is unreasonable to assume that county governments, who are less prepared for data breaches, or their investors, would be in a better position to respond to attacks before an announcement than corporations. Second, there is no reason for the municipal bond market to price a targeted county's bonds as if an attack already occurred before the county notifies the public of the breach, especially because targets have incentive to conceal details until they are legally obligated to report them (Amir et al., 2018). Lastly, although I cannot deny that some attacks are potentially nonrandom, I previously show in **Table 2** that there is no consistently strong predictor of county data breaches, including municipal cash-flow-related variables and urban status. If hackers are not clearly motivated by a county's financial standing or dissuaded by a county's apparent ability to defend against an attack, then it is likely safe to assume that municipal data breaches are the result of hackers randomly succeeding in breaching a target's defenses. Nonetheless, my financing models control for a handful of county characteristics that are marginally associated with the propensity that hackers may choose to target a certain county, thereby reducing the influence of any potentially unobserved confounding factors. As such, β_1 is the difference-in-differences estimator and may be interpreted as the average treatment effect on the treated.

3.3. Term Structure of Cyber Risk

The heterogeneity of municipal bonds' term structure can reveal how investors price expected cyber risk across bonds of different maturities and hint towards when investors think the effects of attacks will be concentrated. It is not immediately clear whether investors should suspect cyber risk to be more of a short-term or longer-term risk for municipalities, though. On one hand, many targets of cyberattacks are affected only temporarily. Kamiya et al. (2021) show that targeted firms do not suffer reduced profitability within the three years after an attack but do experience significant market value loss in the three days surrounding an announcement breach. Similarly, targeted counties may resume their cash flow-generating activities quickly after an event if the breach is not too severe. Alternatively, cyberattacks may have lasting repercussions for targets. For example, Akey et al. (2021) show that targeted firms steadily increase their charitable giving post-attack to restore the value of their corporate reputation, and Tosun (2021) shows that targets change their firm policies up to five years after an attack. Additionally, many cybersecurity experts believe attacks will become more frequent and devastating over time (Brooks, 2022). This ambiguity regarding the relevance of cyber risk over time contrasts other risk factors, like the immediacy of losing wetlands or long-term nature of climate risk (Painter, 2022; Rizzi, 2022).

To identify investor expectations regarding cyber risk, I estimate Eqn. (1) in a stacked difference-in-differences framework on three different subsamples of municipal bonds based on the length of their maturities for each of the dependent variables in **Table 4**. I define short-term bonds as those with maturities less than 3 years, mid-term bonds as those with maturities between 3 and 10 years, and long-term bonds as those with maturities greater than 10 years. Each

estimation includes the same control variables and fixed effects as described in the previous section.

I find that investors require premiums for bonds of only the longest maturities. For example, the initial offer yields on targeted counties' long-term bonds increase 4.1 bps after a cyberattack, but there is no effect for bonds of short- and mid-term maturities. A similar pattern exists when *Spread* and *Adjusted Spread* are the dependent variables. Targeted counties' long-term bonds increase their spreads and tax-adjusted spreads by 13.0, and 18.1 bps, respectively; but shorter-term bonds seem relatively unaffected by cyber risk. The results suggest that investors believe cyber risk is more of a long-term threat to county cash flows rather than a short-term threat. To add evidence to such a claim, I further test and find that the coefficients estimated on the long-term samples are statistically greater than the coefficients on the short-term samples. Investors require a cyber risk premium on only long-term bonds, implying that investors believe the full repercussions of cyberattacks will primarily affect municipal outcomes in the long run.

The interpretation underlying these results is intuitive. My results suggest that investors believe the effects of cyberattacks will stick around after a breach, but the adverse effects will manifest only in the distant future. Stated differently, investors weigh the immediate repercussions of an attack with less importance than they do the longer-term consequences of the attack and the targeted county's associated responses. The results also imply that investors do not believe government cyber defense will ever completely mitigate cyber risk, a thought consistent with those of cybersecurity professionals.¹¹

¹¹ See "Three Reasons Why the Cybersecurity Industry May Never Catch up to Cybercrime," *Forbes*, August 31, 2017.

There are likely two potential reasons such a response is rational. First, investors may think that being targeted once implies that a targeted county could be easily breached again because its attention is focused on recovery and not protection from future events. Repeat attacks are concerning in corporate settings because they are associated with even greater shareholder value loss, but repeats would be especially troublesome for municipalities if the events lead to prolonged periods without the collection of cash flows or to civil unrest arising from reduced public services (Kamiya et al., 2021). Because only Los Angeles County is targeted more than once in my sample, though, any statistical inferences regarding first and subsequent attacks are limited.

Alternatively, investors may believe that the repercussions of an attack, such as the financial or economic costs, will not be fully realized until an indeterminant time in the future. For example, the financial losses associated with an attack may occur all at once or may drag out over many years, like Target’s 2013 data breach.¹² If counties face financial losses, they may be forced to make uncomfortable decisions, such as cutting public programs or raising tax revenue, to offset the direct costs of an attack, even if such actions are associated with adverse economic outcomes (Gundersen et al., 2011; Gao and Zhang, 2017; Vakili and Zhang, 2018; Jackson et al., 2021). Because there is so much uncertainty regarding the future of cybersecurity and investors do not know exactly how – and when – the repercussions of municipal decisions will play out, investors discount all such probable outcomes in the bonds of long-term maturities. I attempt to more clearly address how cyberattacks are related to the cost of municipal financing in the following section.

¹² See “Target to Pay \$18.5 Million to 47 States in Security Breach Settlement”, *New York Times*, May 23, 2017. Although paying \$18.5 million was one of the last public repercussions of their 2013 data breach, Target had accumulated a very large cyberattack bill up to the settlement over the course of several years. The settlement brought the total cost of the cyberattack up to around \$300 million.

3.4. Connection between Attacks and Other Risks

Both cybersecurity experts and the finance literature suggest that cyberattacks can affect targets by increasing their exposure to certain types of risk, and this subsection aims to identify the channels that link data breaches to increased municipal bond premiums (e.g., Campbell et al., 2003; Tanimura and Wehrly, 2015; Amir et al., 2018; Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Ashraf, 2022). I test three aspects of municipal bond risk, discuss the evidence regarding each channel, and conclude the section by documenting the real effects of cyberattacks on targeted counties.

3.4.1. Credit Risk

Data breaches could increase targeted counties' credit risk by prompting rating agencies to lower future bond ratings. Rating agencies may lower county bond ratings if they believe the costs associated with an attack could hinder a targeted county's ability to repay investors (Kamiya et al., 2021). Additionally, targeted counties may find it more difficult to sustain their issuance amounts after an event because of the higher costs associated with the threat of default.¹³

I first examine the effect of cyberattacks on the bond ratings of new municipal issues by estimating Eqn. (1) with *Max Rating* as my dependent variable and present the results in Model 1 of **Table 5**. I find strong evidence that rating agencies downgrade targeted counties' ratings on new issues post-attack. The ratings on targeted counties' new bonds issued after an attack are a little under one-fifth of a letter grade (0.18 points) worse than those of comparable bonds issued by non-targeted counties. Given that the average bond in my sample is rated a 2.87 (AA on the

¹³ See "Cyberattacks Heighten Credit Risks in U.S. Public Sector: S&P", *Reuters*, August 22, 2018, and <https://www.pullcom.com/newsroom-publications-Public-Finance-Alert-Investor-Rating-Agency-Interest-Cybersecurity-and-Climate-Change-Disclosure-Municipal-Bond-Issuances>.

S&P and Fitch scales), one attack would bump down the average bond rating from AA to AA-. These results imply that rating agencies believe attacks significantly increase a county's credit risk.

I next examine if attacks affect a county's primary market issuance activity and present the results in Model 2 of **Table 5**. I aggregate the yearly issuing activity of each county in my sample (*Total Issuance*), transform it by the natural logarithm, and drop counties that have no issuance activity (though my results do not change if I take the logarithm of one plus the data). I use a county-level stacked difference-in-differences framework similar to Eqn. (1), except I include only the county characteristics as control variables. I find that targeted counties decrease their issuance activity about 6% after an attack. However, this difference is not statistically different from zero. As such, I conclude that targets do not differ from non-targeted counties in their primary market issuing activity after an attack.

Altogether, these results suggest that attacks appear to increase county credit risk, but the rating downgrades do not disrupt total primary market issuing activity. Instead, targets choose to finance similar levels of debt post-attack as they did pre-attack but at higher interest rates.

3.4.2. Investor Beliefs Regarding Cash Flow Risk

Counties pay interest on municipal bonds from funds in general obligation (i.e., funds from taxes or intergovernmental sources) or revenue accounts. Revenue bonds are generally considered riskier investments because a county's ability to repay them is tied to a specific project's cash flow (Cestau et al., 2019). However, it ex ante unclear which subset of bonds will be more affected by cyber risk because cyberattacks can affect funds from projects or those in general obligation. The events could decrease targeted counties' cash flows by either reducing

their general obligation funds or preventing them from collecting revenues.¹⁴ The impact on cash flows via either channel could impede the targeted county's ability to repay its bonds, so it is unclear which possibility might pose a greater threat to county cash flows. As such, I exploit the dichotomous nature of general obligation and revenue bonds to identify which possibility investors believe is going to pose a greater risk to county cash flows.

To test the relationship between cyberattacks and investors' beliefs regarding county cash flow risk, I separately estimate Eqn. (1) on subsets of general obligation ("GO") and revenue ("REV") bonds and present the results in **Table 6**. I find that investors require premiums only for revenue bonds issued by targeted counties. In fact, none of the models estimated using the GO bonds produces a statistically significant coefficient on β_1 . Models 1 and 2 show that initial yields for targeted revenue bonds are 9.3 bps higher post-attack, whereas initial yields for targeted general obligation bonds are (insignificantly) 0.006 bps higher than non-targeted general obligation bonds post-attack. Models 3 and 4 tell a similar story regarding spreads. Investors require premiums on targeted counties' revenue bonds that are 20.4 bps higher post-attack, but they do not require a premium for targeted GO bonds. Model 6 further shows that investors require a premium that is, on average, 26.7 bps greater than the after-tax spread over a maturity-matched Treasury for bonds issued by a targeted county post-attack. This premium on revenue bonds represents an almost 12% increase in costs, relative to the mean of *Adjusted Spread*. Investors appear to more heavily weight cyberattacks' potential impact on county revenues.

Initially, it may be surprising that general obligation bonds are not associated with as large a premium as revenue bonds given that the largest costs related to an attack, such as ransom payments or legal fees, would be paid out of general obligation funds. However, such large fees

¹⁴ A targeted county's general obligation funds may be affected if taxpayers relocate to safer counties or if they are forced to pay large legal or professional fees to recover from an attack.

would likely also be covered by a cyber insurance policy, which would possibly not cover lost revenues from services because of a data breach.¹⁵ Even if a targeted county does not have any cyber insurance coverage, it still has greater control over general accounts and can choose to repay general obligation bonds by reallocating funds across different public services, though such a decision may be associated with additional reputation risk.

Although these results are consistent with news reports that describe how attacks have crippled public systems for weeks at a time and prevented government entities from collecting revenues from public services, these subtests do not explicitly show that breaches truly increase cash flow risk.¹⁶ At a minimum, my results show that investors believe the attacks increase bonds' cash flow risk, especially for revenue bonds. However, what investors believe about cyberattacks may not necessarily coincide with what is actually true about cyberattacks (Kvochko and Pant, 2015). Only a more robust test of county cash flows can identify if attacks adversely affect their coffers. I formally test the impact of attacks on county revenues in the following subsection.

3.2.5. Cash Flow Risk, Reputation Risk, and Real Effects of Attacks

Cyberattacks are associated with non-trivial costs to targets, and the breaches can adversely affect future outcomes, such as firm output or reputation (e.g., Amir et al., 2018; Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Tosun, 2021). These risks are paralleled in municipalities, albeit with some nuanced differences. Similar to their effect on corporations, attacks may adversely affect county cash flows if the data breaches are associated with large legal fees, reduced revenue collections, or ransoms. However, a county's reputation

¹⁵ See <https://www.thezebra.com/resources/car-insurance/what-is-cyber-insurance/#infographic>.

¹⁶ See “8 Cities that Have Been Crippled by Cyberattacks — and What They Did to Fight Them”, *Business Insider*, January 27, 2020.

risk from an attack will likely manifest differently than a corporation's risk. Whereas the repercussions of cyberattacks for firms are generally limited to the target and possibly its immediate peers, municipal cyberattacks have the potential to affect societal outcomes (e.g., Huang and Wang, 2021; Ashraf, 2022; Crosignani et al., 2023; Florakis et al., 2023). Counties may be faced with the decision to make unpopular budget cuts that harm their reputation to offset the costs of attacks. Although budget cuts may temporarily help counties recover post-attack, the actions may have adverse longer-run economic consequences and might make it difficult for targets to attract future residents or corporations (e.g., Gundersen et al., 2011; Gao and Zhang, 2017; Vakili and Zhang, 2018; Jackson et al., 2021). Alternatively, attacks may have no effect on county cash flows or reputation.

I formally test the cash flow and reputation channels in a longer-run stacked difference-in-differences setting with data from 7 years before to 7 years after an attack.¹⁷ I use the following model:

$$y_{i,t} = \beta_1 Target_i \times Post_t + \beta_2 Target_i + \beta_3 Post_t + \gamma' Controls_{i,t-1} + \omega_{s,e} + \varphi_{t,e} + \varepsilon_{i,t}, \quad (2)$$

where the dependent variables are taken from two sets of popular county-level per capita budget variables. The first set includes county *General Revenue*, *Total Charges and Miscellaneous Revenues*, *Sinking Fund*, *Insurance Trust Funds*, *Total Cash*, and *General Expenditures* and represents several aspects of county cash flows. The second set includes total county spending on *Police Expenditures*, *Health Expenditures*, *Elementary Education Expenditures*, *Natural Resource Expenditures*, and *Public Welfare Expenditures* and identifies how counties choose to fund their primary social or public works programs. I transform each cash flow and expenditure

¹⁷ I focus on counties that report their account and spending balances every year. I choose the (-7,7) window to maximize the comparison between a longer-run real economic analysis and investor expectations of future outcomes around the majority of events in my sample. However, my results are qualitatively unchanged if I decrease the window size.

variable by the natural logarithm to interpret β_1 as the expected percentage change in y after a cyberattack. My controls include the same county-level controls from previous tests. I include county-event ($\omega_{s,e}$) and year-event ($\varphi_{t,e}$) fixed effects as dataset indicators to force my comparisons within the same county, year, and attack event (Baker et al., 2022), but I also check for robustness to the general size of a county with the addition of county size-decile fixed effects in later tests.¹⁸ Eqn. (2) captures how county cash flows and spending decisions change surrounding an attack. I drop observations that do not report data in the respective accounts to ensure my analysis is not skewed by a small sample of reporting counties. If cyberattacks lead to adverse cash flow-related outcomes or social program budget cuts for targeted counties, then β_1 should be negative to represent that county-level cash flows or spending decreases after an attack.

I present the results of Eqn. (2) on the county cash flow proxies in **Table 7**. Panel A presents the results with county-event and year-event fixed effects, and I include the size decile-event fixed effects in Panel B for robustness. Cyberattacks significantly decrease county cash flows in the period following a breach. For example, targeted counties' general revenue decreases 10% after a data breach, equating to an annual loss of \$23.5 million for the average county. Additionally, cyberattacks affect revenues from charged services and projects by about 10.8% in the period after a breach, and counties deplete their insurance trust fund accounts by about 22.5% and sinking fund accounts (i.e., the account that holds funds to pay off debt) by over 40%. In response to decreased revenues, targeted counties also decrease their general expenditures by about 7%, \$22.7 million for the average county, after a breach. Interestingly, the difference between the expected decreases in revenues and expenditures is about \$857 thousand,

¹⁸ I thank an anonymous referee for this suggestion.

close to the expected increase in the cost of debt for targeted counties computed in Section 3. Each of these results holds when I include the size-decile fixed effects. These results imply that counties adjust their expenditures to account for the potential increase in the cost of debt and loss of revenues.

If cyberattacks affect all aspects of county cash flows, why do investors appear to believe that cyberattacks will primarily affect bonds supported by revenue accounts and not GO bonds? Because all county revenues decrease and not just those associated with revenue-bearing projects, it seems there is a mismatch between what investors believe will happen to a target's underlying cash flows and what actually happens (Kvocho and Pant, 2015). However, the absence of a cyber risk premium in GO bonds could still be rational because funds in general obligation could be insulated by cyber insurance policies. Likewise, counties can reallocate funds across accounts and cut general expenses. Such options provide the opportunity to pay off GO debt and keep the overall risk associated with GO bonds lower than the risk associated with revenue bonds (even though the total pool of funds is smaller).

I next analyze how targeted counties adjust their social and public works spending post-attack in **Table 8**. Panel A presents the results for my main specification, and Panel B includes size decile-event fixed effects as before. I find strong evidence that targeted counties substantially cut spending on policing, public health, elementary education, and natural resources. Targets modestly reduce their budgets for police departments by about 7%, public health by 12%, and elementary education by 8% post-breach. In contrast, targets greatly reduce their environment-related spending by almost 40% after a cyberattack. I also find evidence that targets reduce the size of their welfare safety nets by about 3% after a breach after accounting for the general size of a county. Despite how county budgets traditionally remain stable over time,

these results indicate that cyberattacks lead targets to make significant cuts to their social and public works spending, a fact evinced by a number of news reports that discuss budget challenges post-attack.¹⁹

Altogether, my results portray an interesting picture regarding the real effects of cyberattacks for targeted municipalities. Attacks directly depress targets' cash flow across several dimensions. Although data limitations prevent me from estimating the effect of attacks across a window that corresponds with the full maturity of long-term bonds, it is difficult to reason that targeted counties' cash flows would stop suffering in the period after my estimation window for a couple of reasons. The first is that the direct costs associated with cyberattacks (e.g., litigation, regulatory, or identity theft protection fees) may not necessarily end after the seven-year post-attack period, as evinced by Target's prolonged struggle after its 2013 data breach. The second is related to the possibility of county reputation risk.

Targets make substantial cuts to traditionally important social and public works programs, despite budget cuts being generally unpopular with stakeholders.²⁰ Similarly, limiting public programs could lead to sub-optimal societal outcomes, tarnish a county's reputation as being labor- or business-friendly, and reduce local firm value or innovation (Gundersen et al., 2011; Gao and Zhang, 2017; Vakili and Zhang, 2018; Jackson et al., 2021). However, reputational damage is unlikely to occur all at once, especially if a county sustains its budget cuts in various forms over several years. To illustrate how budget cuts occur over my sample period, I plot the relative timing trends for each of my cash flow and social spending variables in

¹⁹ There are several examples of government budget changes post-attack. See "Sonoma County Tourism Trims Costs, Looks Forward to Reviving Travel", *North Bay Business Journal*, October 6, 2021; "Oregon Lawmakers Reduce Planned Funding for Cybersecurity by Millions" *Oregon Capital Chronicle*, June 22, 2023; and "Cybersecurity Experts Weigh in on Fulton County Government Cyberattack, *11alive.com*, January 30, 2024, for recent examples.

²⁰ See "Few Americans Support Cuts to Most Government Programs, Including Medicaid", *Pew Research Center*, May 26, 2017, for survey results regarding federal budget cuts.

Appendices A and B from three years before a breach to seven years afterwards. As seen in Appendix A, the effects of cyberattacks on most of the revenue accounts are quick and long lasting. Appendix B, in contrast, illustrates a type of pecking order regarding social budget cuts. Counties are quickest to make substantial cuts to health and natural resource expenditures, and they sustain the reductions over my entire sample horizon. Counties likewise reduce police spending after a breach, but they seem hesitant to reduce police budgets to the same intensity as they do health and natural resource spending. In contrast, counties are most hesitant to reduce education and welfare budgets, making most of their adjustments to these accounts within only a couple of years.

Given that there are more immediate consequences for municipal revenues and budgets post-cyberattacks, it is curious why investors require only a long-run cyber risk premium. Counties appear to find a new equilibrium with their budgets given the new constraints introduced by cyberattacks, which minimize any additional risk in the short- or mid-run. However, the repercussions of reputational damage may take even longer to be seen and could indirectly lead to reduced cash flows at any point in the future if businesses and residents choose to locate in, or industries partner with, areas of stronger reputations.²¹ Such concerns are especially relevant given that survey evidence shows that government cyberattacks cause the public to lose confidence in the future efficacy of their elected leaders (Shandler and Gomez, 2023). The long-run risk of targeted municipalities is greater because they adjust their budgets in such a way that threatens how investors perceive the long-run competitive edge of the county. Attacks increase municipal reputation risk and, ultimately, stakeholder uncertainty regarding the future of targeted municipalities.

²¹ In unreported results, I find that targets suffer a reduction in tax revenue, potentially picking up some of this effect.

4. Robustness Tests

In this section, I briefly approach three concerns with my methodology. The first concern pertains to the generalizability of my results given the restrictions I put on my samples of attacks and bonds. The second centers on the construction of my control group. I address both concerns by reproducing the main results with county-event fixed effects in **Table 3** using the same stacked difference-in-differences framework as before but with modifications that address potential criticisms. The final concern centers on the robustness of the stacked difference-in-differences methodology, and I address it by reproducing the main results from **Table 3** with the methodology proposed by Callaway and Sant’Anna (2021).

4.1. Generalizability of Main Financing Tests

One criticism of my methodology is that I ignore potentially valuable variation in local borrowing costs surrounding cyberattacks by excluding attacks on cities. Excluding city bonds, as such, prevents me from generalizing my results. If cyberattacks adversely affect local borrowing costs, then I should observe the effect in a sample of all local bonds. I address the generalizability of the financing tests by including city bonds, and attacks on targeted cities, in the sample and reproducing my main results. Similar to my main definition of *Target*, I assume that all bonds issued by targeted cities are “treated” and all bonds issued by non-targeted cities in the same state and year are the counterfactuals. I match city bonds from SDC to events in the PRC database by name and state of issuer. The inclusion of city hacks allows me to incorporate 23 more events and 154k more bonds.

I present the results of the first robustness test in Panel A of **Table 9**. I find that the relationship between cyberattacks and municipal financing costs still holds after including city bonds. Cyberattacks increase the future spreads of targeted municipalities’ new issues by 11.3

bps, similar to the original point estimate of 12.6 bps. Targeted municipalities' tax-adjusted spreads are 15.5 bps higher than those of their counterfactuals in the same state and year, which is also quantitatively similar to the original estimate of 17.8 bps in **Table 3**. My results are generalizable to all levels of local financing.

Relatedly, my main results could be influenced by contemporaneous events that affected Los Angeles (LA) around the times of its hacks. For example, the city of Los Angeles suffered credit rating downgrades in 2010 and 2013, both of which could influence the market's perception of the county's creditworthiness and may taint the estimation of the ATT around the latter two LA county events. Furthermore, including three hacks that target LA may sway the sample towards LA's bonds given that the county is the most populous in the United States. To address the concern that the LA events introduce endogeneity and sample selection bias into the estimation of the main result, I repeat my main analysis from **Table 3** but exclude the latter two LA hacks and present the robustness check in Panel B. Although the coefficient on *Yield* loses statistical significance, the coefficients on *Spread* and *Adjusted Spread* retain statistical significance and are nearly identical to those estimated in Models 4 and 6 of **Table 3**.

The main results in **Table 3** could likewise be driven by my exclusion of bonds with negative spreads and tax-adjusted spreads. Censoring those bonds out of the sample may remove valuable variation that would otherwise apply downward pressure on the estimated coefficients and lead to inferences that do not reflect municipalities' true costs of financing. I address this criticism in Panel C by including bonds with negative spreads and tax-adjusted spreads in Models 2 and 3. I find that coefficients on *Spread* and *Adjusted Spread* represent a 17.2 bps and 19.0 bps increase in costs, respectively. Although the coefficient on *Spread* is larger than the one

presented in **Table 3**, the coefficient on *Adjusted Spread* is almost identical to its counterpart in **Table 3**. My treatment of negative spreads does not seem to drive my results.

4.2. *Alternative Counterfactuals*

A second criticism of my methodology is the construction of my control group. I employ two alternative approaches to constructing my controls. First, instead of using all non-targeted counties within a state as controls, I use only non-targeted neighboring counties. This difference in the construction of the control group may better account for the influence of any unobserved factors, such as geography or industry concentration, on the cost of municipal financing and may yield more accurate estimates. If cyberattacks truly affect government financing and societal outcomes, then the effect should exist when contrasting targets with their geographical neighbors.

To compare treated counties to their counterfactuals, I use the Census Bureau's county adjacency file to identify neighboring counties of targets within the same state and repeat the main analysis. The sample size decreases to a total of 132k bonds but makes the treatment and control groups more evenly sized. About 44% of the alternative sample are targeted bonds, as opposed to 12% in the main sample. Panel D in **Table 9** presents the results with alternative counterfactuals. I find that the main result still holds after comparing targeted counties with their neighbors. Post-attack, targeted counties suffer higher initial offer spreads (tax-adjusted spreads) that are 12.8 (16.0) bps higher than their neighbors' in the same year. These estimates are also quantitatively similar to the original estimates in **Table 3**.

Next, I use a propensity score matching algorithm to identify control groups in Panel E. I estimate the likelihood that a county is targeted as a function of the natural logarithm of one plus its lagged total revenue, total income taxes, total cash, logged population, logged per capita

income, and logged employment and an indicator of its urban status. I match targets to controls in the same state and year within a 15% caliper, sample with replacement, and take two matched control observations to increase sample size and variation. I use the natural logarithm of *Population*, *Per Capita Income*, and *Employment*, instead of following the exact determinants specification in **Table 2**, to improve my number of matches. As with the previous alternatives, the main result still holds, though with greater magnitudes. I find that targeted counties face offer yields (spreads) that are almost 16 (23.3) bps higher than their counterfactuals'. However, any inferences based on this test should be interpreted with caution because of the limited number of matches. Although I allow for a generous caliper in the propensity score match, only a handful of targeted counties find appropriate matches because of my county size restriction. This limitation severely restricts the sample size used in the estimation and produces point estimates that are likely not reflective of the true average treatment effect on the treated.

4.3. Alternative Approach to Dealing with Heterogeneous Treatment Effects

The final criticism I address focuses on limitations potentially imposed by the stacked difference-in-differences estimator. The stacked difference-in-differences estimator may be considered less stringent or flexible than other alternatives to the staggered difference-in-differences estimator (Baker et al., 2022). As such, I check my preferred model's robustness to the methodology proposed by Callaway and Sant'Anna (2021) with a similar set of control variables to my main specification. I use bonds over the entire sample period from never treated counties as control observations and estimate probability weights in the first stage via OLS regression. I weight the Callaway and Sant'Anna (2021) ATT over a seven-year event window (i.e., from three years before an attack to three years after an attack) to be comparable to the primary stacked difference-in-differences specification.

I present the results in Panel F of **Table 9** and find that my main results largely hold. Model 1 produces a coefficient that is statistically insignificant from 0, but Models 2 and 3 produce coefficients that are similar in magnitude to those produced by the stacked difference-in-differences estimator. Cyberattacks increase the tax-adjusted spreads of targeted counties new issues by about 20 bps after a breach. Even under alternative methodological approaches, the data show cyberattacks increase local financing costs.

5. Conclusion

This paper is among the first studies to link cyberattacks to municipal financing costs and the first study to show how cyberattacks affect long-run county outcomes. I show that attacks substantially increase local borrowing costs, and I link the increase in costs to greater credit, cash flow, and reputation risk post-attack. Investors' expectations of cyber risk do not vary much across the short- and mid-term, but investors appear to believe the worst repercussions of attacks are concentrated in the long-run. Such a concern is reflected in my county-level tests that show attacks adversely affect targets' cash flows and lead targets to make budget cuts that could lead to even worse economic outcomes in the future. My results are robust to numerous sample and econometric specifications, assuaging concerns that they are not generalizable.

My study has important implications for policymakers and investors alike. Unlike other forms of risk, such as natural disaster or climate risk, every county is a potential target for a cyberattack. Unfortunately, potential targets can rarely do much to prevent a hack, especially given that municipal cyberattacks appear randomly distributed. However, counties can still proactively take relatively simple measures to minimize an attack's damage. For example, municipal governments can purchase an additional cyber insurance policy to cover their immediate financial costs related to an attack. Similarly, municipalities can make it a priority to

have an offline backup of all their important systems and data. Doing so would allow governments, if ever targeted, to restore their network more quickly in the event a hacker takes their systems offline or holds their network for ransom. Additionally, governments can upgrade their hardware and hire more skilled cybersecurity experts to reduce the likelihood of a successful attack. Finally, investors can actively encourage municipal governments to utilize updated data security techniques to prevent future attacks from causing lasting damage. Taking even such simple actions can help prevent governments – and their stakeholders – from succumbing to any chronic consequences of the “cyber” bug.

Chapter 2 – Data Breach Information, Hospital Financing, and Patient Outcomes

Abstract

I examine the costs and real effects of medical data breaches using a stacked difference-in-differences research design. I find that data breaches increase the cost of healthcare financing and examine three mechanisms that link breaches to increased costs. While data breaches increase issuer credit risk on average, only hacks – the worst events – harm both hospital and patient health. Yet, investors do not require an incremental premium for bonds of hacked issuers. I find evidence this mispricing is further influenced by levels of investor attention. Altogether, my results suggest that investors do not appropriately price the affected securities.

1. Introduction

Hospitals are crucial organizations in modern life. Not only do they offer a wide array of preventative and emergency care services to patients in all stages of life, hospitals are major sources of revenue and employment in the local economy (MacDorman and Declercq, 2019; CDC, 2020; AHA, 2022). Given the sensitive nature of the data that hospitals hold and the reach of hospitals' role in society, it is no surprise that they are targets of an ever-growing number of cyberattacks that threaten the economic and nonpecuniary benefits that hospitals offer society. For example, the 2021 ransomware attack on the non-profit Scripps Health system in San Diego reduced patient access to medical care during the breach and lost the hospital system over \$100 million, primarily through litigation and lost revenue (Burky, 2023). Despite the potential for breaches to harm wider society, little is known about how the average data breach affects hospitals or their stakeholders. In this paper, I examine how data breaches affect the healthcare market by identifying how they influence both hospital financing and patient outcomes.

Hospital data breaches serve as a unique setting to study how much data breaches cost in both financial and societal terms. First, healthcare data breaches in the United States are subject to federal Health Insurance Portability and Protection (HIPAA) reporting requirements and, consequently, are much less likely to suffer from sample selection bias than breaches of publicly traded firms. As such, a study of hospital breaches is not constrained to just hacks or events that happen after a state passes its own data breach notification laws (e.g., Huang and Wang, 2021; Jamilov et al., 2021; Kamiya et al., 2021). Relatedly, information about breached entities is cleanly identified and is simple to match to external databases because the processes following health-related data breaches are federally regulated. Lastly, the information environment surrounding health-related breaches uniquely contrasts that of corporate breaches. Whereas

information about health breaches is released quickly, hospital performance and patient outcome data is sometimes released with significant delay, potentially taking one to two years for investors to gain access to the information. These unique characteristics allow me to include every type of internal and external health-related data breach, cleanly match them to issuer- and hospital-level data, and test the role of information asymmetry in the pricing of data breaches (Amir et al., 2018). If breaches lead to adverse financial or patient outcomes, then investors should price any associated risks into the cost of hospital financing and breached entities should have worse prospects than non-breached ones. However, any pricing effects may be delayed if relevant information takes time for investors to process or if investors do not understand the information (Ablan et al., 2016; Mayer et al., 2021).

My primary identification strategy exploits the staggered timing of 82 data breaches on U.S. hospitals and compares breached hospitals to non-breached hospitals within the same state and year. Because recent research suggests that staggered difference-in-differences specifications may suffer from biases arising from heterogeneous treatment effects over time, I employ a stacked difference-in-differences specification to overcome possible heterogeneity in my estimation of the average treatment effect on the treated over time (Baker et al., 2022). My sample of events includes the near universe of breaches of hospitals that either issue bonds or report their performance to the Centers for Medicare and Medicaid Services (CMS). Given that the propensity for a hospital to be breached is not strongly correlated with observable characteristics that may influence the likelihood of a breach, my identification strategy allows me to identify the impact of data breaches on hospital outcomes using over 80 quasi-natural experiments.

I begin my primary analysis by examining the relationship between data breaches and hospital financing costs and find that breached hospitals suffer higher costs on new issues. Specifically, breached hospitals face offer yields (spreads over maturity-matched after-tax Treasury rates) that are 39.1 (65.0) basis points (bps) higher after a breach. This represents a 12.0% (21.1%) increase in financing costs, an increase of over \$2 million over the average maturity, after a data breach. The cyber risk premium is 50% greater than the effect of Medicaid expansion on rural hospital yields and twice as large as the effect of opioid abuse on general obligation bond yields (Cornaggia et al., 2021; Gao et al., 2022). Timing tests further indicate that the bond costs of breached and non-breached issuers exhibit parallel trends before a breach, and the increase in financing costs is delayed until investors can determine the financial repercussions of a breach for the issuer. These results are robust to the inclusion of county-level control variables; alternative econometric and sample construction specifications, such as using the staggered difference-in-differences estimator proposed by Borusyak et al. (2023); coarsened exact matching on bond characteristics; and constructing the control group with only non-breached hospitals in the same county as the breached hospital. My results suggest that the market prices cyber risk and the premium is economically significant.

Credit rating agencies appear to have the same reservations towards breached issuers as investors do. I find that new offers by breached issuers are about 2.5 notches lower post-breach. Given that the average bond rating in my sample is BBB on an S&P scale, a data breach would downgrade the average breached hospital's bond to BB+, from investment grade to non-investment grade, holding all else equal. Furthermore, the downgrades appear to be concentrated in the year of a breach announcement and the years after hospital performance data is released. This result is consistent with real-world rating downgrades post-breach and the practical

emphasis that agencies place on the potential governance and cash flow implications of breaches (Mitchell, 2021; Muolo, 2022). As such, credit ratings appear to be one channel through which data breaches influence issuer financing costs.

The timing of the bond cost and rating results suggests that the primary municipal bond market responds to data breaches primarily only after some level of information is released. However, as previously noted, the period between HIPAA-related data breach notifications and the public release of information related to underlying issuer fundamentals is marred by uncertainty, implying that investors are ultimately left on their own to assume how breaches might affect future issuer cash flows. I exploit this setting by examining how investors incorporate additional information that a breach is a hack (which is generally considered the worst type of breach) into their pricing (e.g., Campbell et al., 2003; Hovav and D’Arcy, 2003; Cavusoglu et al., 2004; Huang and Wang, 2021; Kamiya et al., 2021; Florakis et al., 2023).

Although previous empirical findings show that the market should require the greatest premium for investing in hacked entities, some evidence suggests that the market does not respond any differently to hacks than it would other manifestations of cyber risk, especially if investors are not fully informed regarding cyber risk (e.g., Campbell et al., 2003; Hovav and D’Arcy, 2003; Cavusoglu et al., 2004; Kannan et al., 2007; Kvochko and Pant, 2015; Ablan et al., 2016; Huang and Wang, 2021; Kamiya et al., 2021; Mayer et al., 2021; Florakis et al., 2023). Using a stacked triple differences model, I show that the market *does not* require any incremental premium for investing in hacked hospitals. This finding suggests that investors are potentially apathetic or ignorant regarding the devastating nature of hacks. As such, I proceed to examine whether this unexpected result is potentially influenced by the relative unimportance of hacks for hospitals or stakeholder attention to breaches.

I first consider breaches' effect on hospital health as an additional channel through which they influence yields. If data breaches are costly events for hospitals, then they should be adversely associated with cash flow generating activity and balance sheet performance. Furthermore, hacked hospitals should have the worst outcomes if hacks are truly the worst events (Campbell et al., 2003; Kamiya et al., 2021). Using a triple-differences empirical design, I do not find that breaches are associated with any average decrease in cash flow. However, hacks are, indeed, associated with large cash flow losses, contrary to what would be expected from the previous bond tests. Hacked hospitals suffer a 6% loss in total patient revenue after a data breach, driven by a 10% (5%) decrease in inpatient (outpatient) revenue. One possible reason investors may not require any incremental premium for hacks is because municipal bond investors, primarily retail investors, are limited in their information towards the nuances of cyber risk and apply equal weights to all events reported under HIPAA (Ablan et al., 2016; Mayer et al., 2021; MSRB, 2022). Alternatively, investors may be responding to changes in patient outcomes.

Following Jencks et al. (2009) and Aghamolla et al. (2023), I use hospital-level data on 30-day patient readmission rates and patient surveys regarding their perception of care to examine if investors potentially require higher yields due to worsened patient outcomes. Conditional on admission to a breached hospital, patient care seemingly improves at breached (non-hacked) hospitals but worsens at hacked hospitals after an event. The average improvement in care is potentially attributable to mandatory staff training following a breach, while the worse performance after a hack is likely due to healthcare providers' inability to effectively access systems or equipment used in the modern healthcare environment. Both results are consistent with anecdotal evidence and academic evidence found in the medical literature (Forsetlund et al.,

2021; Dameff et al., 2023; GHP, 2023). Consequently, investors' bond market response to breaches is unlikely a response to changes in care and more likely driven by the final factor I consider.

Lastly, I identify the role that investor and patient attention to news plays in mitigating information asymmetry surrounding hospital data breaches. Motivated by Da et al. (2011), I use Google Trends search volume index (SVI) of news articles that include the phrase “data breach” to proxy for attention around hospital data breaches. I collect SVI on news articles to better account for both the release of information related to cyber risk and potential stakeholder attention to data breaches. I repeat both my main financing test and the test of hospital cash flow generating activity and find that the hospital cash flow results are persistent whether attention on data breaches is high or low. In contrast, the financing result seems driven primarily by activity in high attention periods. Altogether, my results suggest that investors are likely out of tune with the reality of healthcare data breaches unless their attention is already considering breaches.

My paper makes several contributions to the literature. First, it adds to a recent literature on hospital financing costs and, to the best of my knowledge, is the first to discuss the financial and real implications of cyber risk for hospitals (e.g., Cornaggia et al., 2021; Cornaggia et al., 2022; Gao et al., 2022; Aghamolla et al., 2023). I show that data breaches are associated with increased financing costs, large losses in hospital revenue, and credit downgrades. Patient outcomes suffer with the worst events. As such, my results have managerial implications for municipalities. Hospitals would likely benefit from incorporating stronger data protection policies, improving data practices, or retaining with cyber risk experience.

Second, my study adds to the broad literature on the relevance of mandatory disclosures (e.g., Griffin, 2003; Lerman and Livnat, 2010; Christensen et al., 2017; Noh et al., 2019;

Cabazon, 2023). Because of my paper's unique setting, I am able to test how markets incrementally respond to hacks over other types of breaches when clear, federally regulated information about the events is produced quickly by targets who cannot indefinitely delay their reports (Campbell et al., 2003; Amir et al., 2018; Kamiya et al., 2021). My study produces two novel findings. First, hacks, on average, are not incrementally priced in the municipal bond market. Second, this mispricing is likely due to a combination of investor information regarding the relative importance of hacks and investor inattention.

Lastly, my paper also contributes to a recent literature on the repercussions of cyber risk for the stakeholders of breached entities (e.g., Ashraf, 2022; Crosigniani, 2023; Osborne, 2023). Similar to the effect observed in Dameoff et al.'s (2023) case study, hospital hacks likely have a net negative effect on society by harming other hospitals' abilities to provide appropriate care. Relatedly, the increased cost of healthcare financing in municipal bond markets due to investors' cyber risk premium is ultimately borne by local citizens and businesses. Given that I show that municipal bond investors seemingly misplace their risk premiums, municipal bond issuers may find it worthwhile to better differentiate between the effects of hacks and non-hacks when communicating the relevance of the events with investors.

The rest of my paper proceeds as follows. Section 2 describes HIPAA's notification laws and my data, and Section 3 outlines my identification strategy and results. Section 4 provides robustness tests. Section 5 concludes and highlights policy recommendations for government data security.

2. Institutional Details and Sample

2.1. HIPAA Notification Requirements

Passed in 1996, HIPAA is a broad-reaching federal regulation that was designed to modernize how the healthcare industry approaches medical information in a modern age. Although the act addresses a plethora of closely related subjects, such as health insurance and medical savings accounts, HIPAA is now largely synonymous with a patient's right to privacy regarding his or her medical history. Many organizations and providers, from individual doctors to insurance companies, in the healthcare industry are covered by HIPAA and must stringently protect patients' protected health information (PHI). Specifically, PHI is anything in a patient's medical record that (1) was recorded during the provision of a medical service or created during the course of medical research and (2) an external party can use to identify a patient. Regarding the latter, the act explicitly defines 18 categories of identifiers that must be present with health-related information in order for any information to be protected under HIPAA.²² The U.S. Department of Health and Human Services (HHS) enforces HIPAA and can assign both criminal and civil penalties to those who violate a patient's rights. Penalties for violating HIPAA vary with both the intent behind a breach and the severity of a breach, potentially resulting in up to 10 years in prison, a \$1.5 million dollar fine, or a provider's exclusion from participating in Medicare.²³

²² These 18 identifiers include names, addresses, ages and dates, phone numbers, fax numbers, email addresses, Social Security Numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate numbers, vehicle identification numbers and license plate numbers, device identifiers and serial numbers, website URLs, IP addresses, biometric identifiers, full-face photos, and any other unique identifier or code that can identify the person to whom a medical record refers. De-identified medical data, by definition, is not considered PHI.

²³ There are numerous resources that describe HIPAA, PHI, and the penalties associated with violations in deeper detail. However, for a brief primer on the regulation, see the CDC's "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", U.C. Berkeley's "HIPAA PHI: Definition of PHI and List of 18 Identifiers", and the AMA's "HIPAA Violations & Enforcement" online articles. Note that the 2009 data breach notification law is different from the 2003 Security Rule, which established standards to protect electronic PHI. See "The Security Rule", U.S. Department of Health and Human Services, and the Code of Federal Regulations 45, Parts 160 and 164.

HIPAA introduced guidance regarding data breach notifications in April 2009, codified its data breach notification rule (45 CFR §§ 164.400-414) in August 2009, and began to enforce the rule in September 2009. Under the notification rule, a covered entity is to assume that the use or disclosure of PHI is a breach if the security or privacy of the information is compromised unless the entity is able to demonstrate that there is a low probability the PHI was actually compromised. Covered entities may use at least four factors to determine if a breach compromised the integrity of PHI, including: the extent of PHI involved, the identity of the unauthorized person who accessed PHI, whether the unauthorized person actually acquired or viewed PHI, and the extent to which the covered entity has mitigated the risk of a breach of PHI.²⁴ If a covered entity finds that a data breach of PHI has occurred, then the entity must notify several parties of the breach in a timely manner. The breached entity is required to notify the affected individuals via written notice sent by physical mail or email (if the victims have previously agreed to receive electronic communications) no later than 60 days following the entity's discovery of the breach. HIPAA requires the notifications to include details describing the breach, the types of information revealed in the breach, the steps affected individuals should take to protect themselves from harm, what the covered entity is doing to investigate the breach and mitigate the potential harm arising from the event, what the covered entity is doing to prevent further breaches, and contact information for the covered entity. If the covered entity does not have sufficient or up-to-date information for at least 10 individuals, the entity must post an equivalent notice on its website's homepage for 90 days or in print at a newspaper or over

²⁴ There are three exceptions to what HIPAA considers a breach. First, there is no breach if a member acting under the authority of a covered entity unintentionally acquires, accesses, or uses PHI in good faith or within the scope of authority. Second, there is no breach if a member of a covered entity inadvertently discloses PHI to another member of the same covered entity (or associated entity) who is also authorized to access PHI. Lastly, there is no breach if a covered entity has a good faith belief that an unauthorized individual who accessed PHI is unable to retain the PHI.

broadcast media where the individuals are likely to reside. Covered entities must also notify the Secretary of HHS through a standardized online form (OMB 0945-0001), which will then post information about the breach on HHS’s website.²⁵ If a breach involves the loss of 500 or more individuals’ records, covered entities must additionally notify “prominent” media outlets via press releases or other means of mass communication, and HHS will conduct further investigation into the breach.²⁶

HIPAA’s PHI breach notification law is, arguably, the most stringent data breach notification law in the United States because of its strict notification requirements. Although the majority of states passed their own data breach notification laws by 2009, states may differ in both what they consider a breach and how they require breached entities to respond. As such, many corporations have significant leeway in choosing what and when to disclose about their data breaches under state regulations. Furthermore, the U.S. Securities and Exchange Commission, despite issuing guidance regarding the disclosure of cybersecurity risk in 2011, did not officially adopt any requirements for publicly traded companies to disclose events until 2023. The ambiguity surrounding data breach notification laws for non-PHI has allowed firms to either avoid notifying stakeholders of breaches, time their notifications in such a way as to minimize the disruption caused by the breaches, or even trade on inside information regarding breaches while the firm waits to disclose information (Amir et al., 2018; Lin et al., 2020; Kamiya et al., 2021). However, breaches of PHI are not afforded such opportunities because of HIPAA’s notification requirements. Any covered entity located anywhere in the United States who

²⁵ Covered entities may report breaches to the Secretary of HHS involving less than 500 patients’ records on an annual basis but are still required to notify the individuals within 60 days of discovery. Breaches involving 500 or more records must be reported to the Secretary within 60 days of discovery.

²⁶ See “Breach Notification Rule”, U.S. Department of Health and Human Services, and the Code of Federal Regulations 74 FR 42767.

experiences a breach of PHI must follow HIPAA’s notification requirements or be severely punished by HHS.

As is standard in the cyber risk literature, I use the Privacy Rights Clearinghouse (PRC) dataset to collect my sample of breaches (Huang and Wang, 2021; Kamiya et al., 2021; Florakis et al., 2023). PRC collects information on data breaches that are publicly disclosed through government agencies, including HHS. I begin by identifying breached medical providers.²⁷ However, I do not subset my events to include just entities that were hacked or events that involved malicious external actors, as Kamiya et al (2021) propose, because of HIPAA’s 2009 data breach notification requirements. Restricting my sample to include medical events in and after 2009 ensures that my sample does not suffer from selection bias because I employ the near universe of mandatorily reported medical breaches.

2.2. Bonds and Hospitals

I use data from additional sources throughout my analysis. First, I collect municipal healthcare bonds from Mergent for the period 2006 to 2022.²⁸ In addition to bond *Yield*, I additionally proxy for the risk premiums investors demand for investing in municipal bonds with after-tax spreads over Treasuries (Cornaggia et al., 2022). I first compute a bond’s spread as the difference between municipal bond yields and maturity-matched Treasury bond yields, using linear interpolation of Treasury yields when an exact match is unavailable. Then, I compute *Adjusted Spread* as the after-tax spread over Treasuries by using the highest marginal tax rates for a given year.²⁹ Following Aghamolla et al. (2023), I further collect hospital performance data from various CMS programs. Additionally, I obtain patients’ 30-day readmission rates from the

²⁷ The PRC database identifies all breached healthcare entities with the *Type of Organization* flag “MED”.

²⁸ I assume healthcare-related bonds are those with use of proceeds codes “OHCA”, “HOEQ”, “HOSP”, and “NURS”.

²⁹ State tax rates come from <https://www.taxpolicycenter.org/statistics/historical-highest-marginal-income-tax-rates>.

Health Care Reporting Information Systems (HCRIS) and patient satisfaction surveys come from the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) over 2015 to 2022. Hospital financial and balance sheet data come from Care Compare over the period 2011 to 2019. Note that Care Compare is updated with a significant delay, sometimes taking up to two years to reflect a hospital's financials.³⁰ I discuss this unique attribute of Care Compare's data and exploit it in my analysis later.

I further restrict my sample of breaches to those that I can match to the issuers of municipal health-related bonds or hospital performance data. To identify "breached" bonds, I match the names of breached medical providers in the PRC dataset to the names of every bond issuer in the same state and assign a variable *Breach* that equals one to each bond associated with a matched issuer.³¹ Because medical data breaches are reported in a standardized manner, matching medical breaches to breached hospital outcomes is much simpler and cleaner than in studies of corporate data breaches. I identify exact matches between the hospitals in the PRC and CMS datasets and, similarly, assign a *Breach* value of 1 to all hospitals in which I can find a match. Control observations are all non-breached bonds and non-breached hospitals in the same state as a breached entity, and I assign all such observations a *Breach* value of 0. These

³⁰ See <https://data.cms.gov/provider-data/topics/hospitals/measures-and-current-data-collection-periods>.

³¹ There is large variation in the names provided by Mergent. To standardize the list of potential names and aid in matching across datasets, I match each name Mergent provides to each other name associated with the same 5-digit CUSIP number. I use 5-digit CUSIP instead of 6-digit CUSIP to broaden my matches across issuers that are clearly related but received different CUSIP numbers in the application process. For example, the issuers "MONTGOMERY ALA MED CLINIC BRD 1976 EAST HEALTHCARE FAC REV" and "MONTGOMERY ALA MED CLINIC BRD HEALTH CARE FAC REV" have the 6-digit CUSIPS 61305R and 613058, respectively. Matching names based on the 6-digit CUSIP could cause me to assign treatment status to one set of bonds but not the other, although the issuers are clearly the same entity. However, matching on the 5-digit CUSIP 61305 avoids this mis-assignment problem. Furthermore, I assume that each alternative spelling of a name associated with the same 5- or 6-digit CUSIP belongs to the same underlying issuer. Additionally, Mergent sometimes lists cities and counties as the issuers of medical bonds instead of the name of the associated project. Consequently, using only names of breached medical providers would cause me to exclude valuable variation if one of these unnamed providers was breached. As such, I further include the sample of county and city events of Osborne (2024) to identify more issuers of hacked medical bonds, but my main results are robust to their exclusion.

restrictions provide a total of 82 unique breaches. Nineteen are matched to bond issuers, and 63 are matched to hospitals from CMS. For my analyses, I keep all rated bonds issued and all hospital observations within a seven-year window around a breach (i.e., three years before and three years after).

Lastly, I collect county-level data from two sources. First, I hand-collect each issuer's location through an iterative process because Mergent does not include the county location of issuers. I gather an issuer's county either from searching MSRB's Electronic Municipal Market Access (EMMA) system, scraping it directly from the name of the issuer, or searching for the name of the project through online search engines. If I cannot identify an issuer's county through any of the aforementioned steps, I assume that an issuer is located in the state capital and its county is the primary county in which the capital is located. Second, I collect county characteristics, *Population*, *Employment*, and *Per Capita Income*, from the Bureau of Economic Analysis. I match the economic data to bond issuers on county name, state name, and year but use lagged county characteristics in my analysis to avoid possibly endogenous controls.

2.3. Descriptive Statistics and Determinants of Breaches

Table 10 presents summary statistics for the main variables in this study. Panels A, B, C, and D present statistics related to my overall sample of bonds, hospital financials, patient 30-day readmission rates, and patient experience surveys, respectively. Appendix E describes variable definitions. I winsorize all continuous variables at the 1st and 99th percentiles. My total sample includes 11,987 healthcare bonds, about 65k hospital-years of financial data, and about 10k hospital years of patient data. Breached hospitals issue about 7.8% of the healthcare bonds, while hacks comprise about half of the events associated with breached issuers. The average bond in my sample has an initial offer yield of 3.3%, matures a little past 12 years after issuance, and

provides a hospital \$8.83 million in funding. The median total issue size is about \$75.8 million. About 17% of bonds are funded via counties' general obligations, but the majority (83%) are funded via hospital revenues. The average bond is rated about BBB. Overall, my sample of hospital bonds largely reflects the samples of Cornaggia et al. (2022) and Gao et al. (2022); and my sample of hospital and patient data is similar to Aghamolla et al. (2023).

I preface my primary analysis by examining the determinants of hospital data breaches in **Table 11**. I use a linear probability model to estimate the likelihood that a hospital is breached in any given year by conditioning on several factors. I include several lagged, logged independent variables to capture observable characteristics that may influence the propensity a hospital is breached. For example, the variables *Total Revenue*, *Total Assets*, *Total Liabilities*, and *Cash Holdings* all measure a hospital's size, potentially available (i.e., stealable) funds, or ability to pay hackers' ransoms. They also capture a hospital's potential defenses and data security practices under the assumption that larger hospitals with better cash flow could have more resources to devote to stronger data practices. The variable *Full-Time Employees* captures how a hospital's labor force may influence a data breach. Lastly, the variable *Beds* is the number of beds a hospital has and proxies for both the size of a hospital and its potential reputation. Model 1 includes hospital and year fixed effects to control for unobserved time series factors, such as the macroeconomic environment, and cross-sectional factors, such as a hospital's culture towards technological progress that may influence a hospital's propensity to be breached. Model 2 replaces the hospital and year fixed effects with county-year fixed effects to account for any role a hospital's local economic environment could have on data breaches or employees' data security practices.

No one factor is a consistently strong predictor of hospital data breaches. In fact, the only variable with any association with data breaches is *Cash Holdings*, which positively predicts the events only in the model that controls for local economic conditions. According to Model 2, a 1% increase in a hospital's stored cash increases the likelihood of a data breach by 0.05%. No other factor, including hospital revenues or the number of employees, appears to be relevant for the likelihood that a hospital reports a breach to HIPAA. Overall, hospital data breaches appear to be randomly assigned, so I assume that data breaches are exogenous shocks to hospitals for the purposes of my following analyses (e.g., Amir et al., 2018; Kamiya et al., 2021; Ashraf, 2022; Crosignani et al., 2023). Nonetheless, I choose to follow the municipal bond literature and control for a county's lagged population, per capita income, and employment in my bond analyses to account for how these characteristics may affect investors' responses to a breach (Cornaggia et al., 2018; Gustafson et al., 2023). Similarly, I follow Aghamolla et al. (2023) and control for a hospital's lagged total income, bed days, cash holdings, liabilities, and total patient revenue in my hospital analyses.

3. Empirical Strategy and Results

In this section, I examine how data breaches affect hospital financing costs and identify the channels through which the events influence investors. I also document the real effects of breaches.

3.1. Identification Strategy

My primary model is the following stacked difference-in-differences regression specification with three years of pre-breach and three years of post-breach data (i.e., a seven-year window):

$$y_{i,t} = \beta_1 \text{Breach}_i \times \text{Post}_t + \beta_2 \text{Breach}_i + \beta_3 \text{Post}_t + \gamma' \text{Controls}_{i,t} + \omega_{s,e} + \varphi_{t,e} + \varepsilon_{i,t}. \quad (1)$$

My primary dependent variables include *Yield* and *Adjusted Spread* for the municipal financing models. The coefficient β_1 estimates the impact of data breaches on hospital outcomes and is my coefficient of interest. *Breach* is an indicator that equals one if a bond is issued by a breached entity and zero otherwise. *Post* is an indicator that equals one if a bond is issued after a data breach. Following the municipal bond literature, I include several bond and county characteristics as controls. The continuous bond characteristics I include are a bond's coupon rate, maturity, inverse maturity, and corresponding maturity-matched Treasury yield (which is excluded from the *Adjusted Spread* model). I also control for whether an observation is a callable, negotiated, or general obligation bond with respective indicator variables. I also include the prior year's population, per capita income, and employment of the issuer's county to control for local economic factors that may affect an issuer's ability to repay its debts (Cornaggia et al., 2021; Cornaggia et al., 2022). I do not include a bond's rating in my primary analysis because it would be an endogenous control variable, as I hypothesize that credit risk is one of the channels through which data breaches influence the cost of capital.

I use a stacked difference-in-differences specification because standard staggered difference-in-differences models may be subject to biases arising from heterogeneous treatment effects over time. In fact, estimates of the average treatment effect on the treated (ATT) produced via staggered difference-in-differences estimators may even have the opposite sign of the true treatment effect. I overcome this challenge by implementing the stacked difference-in-differences estimator (Cengiz et al., 2019). Following Baker et al. (2022), I structure my data in such a way to create an event-specific dataset for each treatment group and its clean control group to represent a singular "experiment" for each breach. Treated hospitals are those that experience a data breach, and treated bonds are any bonds issued by a breached hospital. Control hospitals are those that are never breached but are in the same state as the breached ones. Next, I "stack" all the breach-specific datasets together. Even though each event happens at a different time, the stacked dataset aligns all the breach-specific datasets together in event-time because I take a sample of bonds within a seven-year window of each event. As such, I essentially have 82

quasi-natural experiments from which to estimate the impact of data breaches on several hospital outcomes.³²

Alongside the stacked difference-in-differences design, I include issuer-event ($\omega_{s,e}$) and year-event ($\varphi_{t,e}$) fixed effects in my primary model to further ensure my comparisons of treatment and control outcomes are within the same issuer-experiment and year-experiment. I choose to cluster standard errors at the issuer-level to account for residuals being correlated within a hospital over time.

My identification strategy exploits variation from multiple sources. First, it relies upon a clean shock to treatment group outcomes. With the inclusion of year fixed effects, my model differences out any unobserved cross-sectional factors that might affect both treatment and control groups simultaneously (Cornaggia et al., 2022). This first difference helps ensure that my estimate of the average treatment effect on the treated, β_1 , is not biased by any omitted variables – such as a general macroeconomic conditions or annual trends in cyberattacks – that might be relevant to either group’s outcomes post-breach. Furthermore, with the inclusion of issuer fixed effects, my model differences out any unobserved time-invariant hospital-specific factors, such as a hospital’s governance structure or workplace culture towards data security, that may endogenously affect a hospital’s financing. Used together, the fixed effects reveal how the cost of financing changes for breached entities after a data breach.

Second, my identification strategy exploits the staggered nature of data breaches. Breaches affect hospitals between 2005 and 2016, allowing me to capture all relevant events over the sample period and mitigate concerns that a singular contemporaneous trend might confound the treatment assignment. Treatment hospitals enter my sample three years before they suffer a data breach and exit three years afterwards, so I observe both their pre- and post-breach financing costs. I assign the breach date of the treated hospital to all non-treated hospitals in the same state because control hospitals do not experience their own data breaches. This allows me

³² Specifically, I have 19 events that I match to issuers in Mergent and 63 that I match to hospitals in CMS’s databases.

to observe all pre- and post-breach outcomes for treated and control hospitals over the same seven-year window centered on the treated hospital's breach. Given that I choose plausible counterfactuals for treated hospitals and control for characteristics that are related to the issuers' ability to repay their debts, this difference-in-differences research design forms a unique experiment that allows me to identify the effect data breaches have on hospitals' cost of capital.

3.2. *Impact of Breaches on Hospital Financing*

I begin by quantifying how data breaches impact hospital financing costs using the dependent variables *Yield* and *Adjusted Spread* in **Table 12**. I find that financing costs increase for hospitals after a data breach. Model 1 shows that treated issuers' initial offer yields are 47.8 bps higher after a breach. With the inclusion of bond- and county-level controls in Model 2, I find that issuer yields increase 44.3 bps after a breach. Economically, this translates to a 14.2% increase in total borrowing costs – about \$2.75 million for the median issuer.³³ This result holds when using *Adjusted Spread* as the dependent variable as well. Model 4 shows that tax-adjusted spreads for medical bond issuers increase 74.9 bps (25.1%, relative to the mean value) after a breach. The cyber risk premium is 50% greater than the effect of Medicaid expansion on rural hospital yields and twice as large as the effect of opioid abuse on general obligation bond yields (Cornaggia et al., 2021; Gao et al., 2022).

My identification strategy and interpretation of the stacked difference-in-differences estimator relies on the parallel trends and exogeneity assumptions of any standard difference-in-differences test. I first test the parallel trends assumption for each of my dependent variables with a dynamic analysis in **Figure 2**. Specifically, I replace *Post* in Eqn. (1) with six indicator variables to capture the subperiods surrounding the year of a breach and, following econometric

³³ I utilize the modified duration approach to calculate the increase in borrowing costs for breached issuers. \$2.75 M = \$75.8 M (median annual issuance) × 8.367 (median duration) × (0.0044/(1 + 0.0327/2)).

tradition, use the year immediately before the event as the reference period. Given that all of the coefficients for the pre-periods are statistically indifferent from zero, I find no evidence that treatment and control bonds follow different trends before a hospital is breached. The relationship between data breaches and financing costs exists solely after a breach. However, the post-event timing is especially interesting because it contrasts the more immediate timing of when cyberattacks impact corporate outcomes (e.g., Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Crosignani et al., 2023). Despite HIPAA requiring hospitals to report breaches within 60 days, the market takes about two years to positively adjust its risk premium for breached hospitals. Intriguingly, the market's delay roughly corresponds to how long hospitals may take to fully report their financial and operational data to CMS (i.e., one-and-a-half to two years). Such a delay implies that there is significant information asymmetry between issuers and investors in the period immediately after a breach, and investors seem to not respond to the average breach until after they can gauge its financial implications.³⁴ I explore the potential roles of information asymmetry surrounding hospital outcomes in later tests.

Additionally, endogeneity is unlikely to be a major concern for my use of the stacked difference-in-differences estimator. First, breaches are always unexpected shocks and, many times, undefendable events for even the largest, best-equipped corporations (Kamiya et al., 2021;

³⁴ One could argue that the market's delayed response is rather the result of delayed data breach notifications by CMS. Theoretically, investors may not receive information about a breach less than a year after the event if (1) the breach affects less than 500 individuals, (2) they themselves are not affected by the breach, and (3) neither the breached party nor the affected individuals notify the broader public or a news source. If all three of the conditions are met, then investors could have no information about potential data breaches until one year has past (i.e., the maximum time a breached hospital has to report an event). Combined with delayed reporting of financial data, investors would still have no picture of how a breach influenced hospital health until one to two years after a breach. However, this scenario does not explain the pattern exhibited in Figure 1. In untabulated tests, I examine whether breaches that affect more than 500 records exhibit the same timing as breaches that affect less than 500 records because markets should respond more quickly to information about the former group, given HIPAA's reporting requirements. I find that investors quickly respond to breaches that affect less than 500 records, suggesting that they do not have to wait long to incorporate new information about the breaches or for CMS to disseminate information about the breach.

Crosignani et al., 2023). It is unreasonable to assume that hospitals, who are less prepared for data breaches with their security resources, or their investors, would be in a better position to respond to breaches before an announcement than corporations. Second, there is no reason for the municipal bond market to price a treated hospital's bonds as if a breach already occurred before the issuer notifies the public of the breach, especially because breached entities have incentive to conceal details until they are legally obligated to report them (Amir et al., 2018). Lastly, although I cannot deny that some events are potentially nonrandom, I previously show in **Table 11** that there is no consistently strong predictor of hospital data breaches, including cash-flow-related variables and hospital size. It is likely safe to assume that hospital data breaches are the random result of either hackers succeeding in breaching a target's defenses or employees failing to practice proper data protection protocols. Nonetheless, my models control for a handful of characteristics that may be theoretically associated with the propensity an event may occur, thereby reducing the influence of any potentially observable or unobservable confounding factors. As such, β_1 is the difference-in-differences estimator and may be interpreted as the average treatment effect on the treated.

3.3. Connection between Breaches and Increased Costs

Both cybersecurity experts and the finance literature suggest that data breaches can affect victims by increasing their exposure to certain types of risk, and this subsection aims to identify the channels that link data breaches to increased bond premiums (e.g., Campbell et al., 2003; Tanimura and Wehrly, 2015; Amir et al., 2018; Akey et al., 2021; Huang and Wang, 2021; Kamiya et al., 2021; Ashraf, 2022). In doing so, I present evidence that investors are not fully informed in their pricing decisions.

3.3.1. Credit Risk

The connection between issuer credit risk and data breaches is straightforward theoretically. Data breaches could increase issuers' credit risk if the events hinder hospitals from promptly repaying their debts. If there is an association between data breaches and credit risk, then breached issuers should have lower credit ratings on new bond issues after their first data breach, relative to non-breached issuers (Kamiya et al., 2021). To test this hypothesis, I conduct a timing test of bond ratings (*Max Rating*) in the same stacked difference-in-differences framework and present the results of a rating timing analysis in **Figure 3**.

Data breaches are associated with significant bond ratings cuts. Although treated hospitals have higher ratings than control hospitals before a breach, I find that credit rating agencies reduce the ratings of new issues by breached issuers by about 2.5 notches post-breach. Furthermore, the rating reduction is constant for the duration of the post-period. Given that the average bond rating in my sample is BBB on an S&P scale, a data breach would downgrade the average hospital's bond to BB+, holding all else equal. In other words, the average hospital with investment-grade bonds should expect to see its bonds drop to non-investment grade after a data breach. Interestingly, the statistical significance of the post-period downgrade appears to be concentrated in the year of a breach announcement and the years after hospital performance data is released (i.e., years 2+). This result is consistent with the magnitude of real-world rating downgrades post-breach and anecdotal evidence that rating agencies emphasize the potential governance and cash flow implications of hospital data breaches (Mitchell, 2021; Muolo, 2022). As such, credit ratings appear to be one channel through which data breaches influence issuer financing costs.

3.3.2. Hacks and the Role of Information Asymmetry

I begin to address the role of information asymmetry in the pricing of data breaches by considering the incremental effect of hacks on breached hospitals' financing costs. Ex ante, it is unclear theoretically whether the hospital bond market should require a larger premium for hacked issuers. On one hand, there are numerous empirical findings that suggest hacks are the worst type of realized cyber risk because they are associated with greater financial losses than other realizations of cyber risk and are, arguably, more likely to be covered in the news because of the reputational damage they cause (e.g., Campbell et al., 2003; Hovav and D'Arcy, 2003; Cavusoglu et al., 2004; Huang and Wang, 2021; Kamiya et al., 2021; Florakis et al., 2023). If investors incorporate all relevant information about breaches into financing costs, then they should require an additional premium for investing in the bonds of hacked issuers.³⁵ As alluded to before, though, some evidence suggests that the market may not respond differently to hacks than it would other breaches. If investors do not have cyber risk expertise, understand that different types of breaches have varying levels of repercussions, or just not pay attention to news, then they may not respond incrementally to hacks (e.g., Kannan et al., 2007; Kvochko and Pant, 2015; Ablan et al., 2016; Mayer et al., 2021).

My identification strategy and sample of data breaches provides the opportunity to uniquely contribute to this debate with a stacked triple-differences test and a sample of all types of data breaches that does not suffer from sample selection bias. The stacked triple-differences test builds upon Eqn. (1) by interacting an additional variable *Hack*, an indicator that equals one for events that are reported as hacks by external parties and zero otherwise, and the existing interaction terms. I include each of the level terms and their interaction pairs to interpret the

³⁵ It is important to note that breached medical providers detail whether they are hacked by an external party in their required reports.

coefficient on the triple interaction as the difference-in-difference-in-differences estimator and present the results of the stacked triple-differences test in **Table 13**.

Contrary to expectations, the coefficient on the triple-differences estimator is not statistically significant in any model, implying that investors do not require incrementally larger premiums after hacks. Instead, the coefficient on *Breach*×*Post* increases in economic magnitude and statistical significance across each model. Models 2 and 4 now imply that hospitals' initial offer yields (tax-adjusted spreads) increase 66.9 (109.1) bps after a breach. Relative to the mean values, the updated estimates reflect a 20.0% (35.4%) increase in yields (tax-adjusted spreads) post-breach.³⁶ Yet, the insignificant triple-differences coefficient may indicate an appropriate response from investors if information indicates that hospital fundamentals are not affected after a hack. I explore two reasons, information about hospital health and investor attention, behind the insignificant relation between financing costs and hacks in later tests.

3.3.3. Hospital Health

Next, I examine the connection between data breaches and hospital health via hospital cash flows. If data breaches are costly events for hospitals, then they should be associated with losses in revenue and the worst outcomes should be reserved for hacked hospitals (Campbell et al., 2003; Kamiya et al., 2021).

I utilize a similar stacked triple-differences methodology as before to test the relation between hospital cash flows and data breaches. Because this is a hospital-level test, my dependent variables of interest are now (total) *Patient Revenue*, *Outpatient Revenue*, *Inpatient Revenue*, and *Bed Utilization*; and each dependent variable is transformed by the natural logarithm of one plus the underlying data. I follow Aghamolla et al. (2023) and include the

³⁶ In Appendix F, I show this effect holds in the secondary market using monthly dollar-weighted average yields as my dependent variable of interest within a seven-month window of a breach announcement.

lagged hospital-level variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. These control variables should mitigate the effect that characteristics like hospital size, access to funding, or cash levels might have on the *Breach* treatment effect. Furthermore, I include data breaches only between the years of 2015 and 2017, due to data constraints from CMS, to ensure that I have a full three years of pre- and post-breach outcomes and hospital-event and year-event fixed effects to parallel my bond-level tests (Baker et al., 2023). I present the results of the cash flow tests in **Table 14**.

Interestingly, I do not find that breaches are associated with any average decrease in cash flow. Instead, hacks are, indeed, the worst type of breach for a hospital to experience. Hacked hospitals suffer a 6% loss in total patient revenue after a data breach, and this effect is primarily driven by a 10% (5%) decrease in inpatient (outpatient) revenue. Additionally, hacked hospitals see a 2.3% decrease in their bed utilization rates post-breach, implying these hospitals generate less revenue on inpatient services and use fewer beds post-breach. These findings are directly opposite those of the bond-level tests that suggest investors care about the presence of any type of data breach but do not incrementally price hacks. There is a connection between data breaches and hospital cash flow risk, but the effect exists only in the subset of treated hospitals for which the market does not require incremental premiums. If bond prices reflect the discounted future cash flows of affected hospitals, it would seem that what investors think will happen does not fully reflect what truly does.³⁷

³⁷ In Appendix G, I consider how data breaches affect hospital balance sheets by following Aghamolla et al. (2023) to measure hospital health with the variables (total) *Assets*, *Liabilities*, *Cash*, and *Fixed Equipment*, each scaled by the hospital's lagged *Total Revenue* and transformed by the natural logarithm of one plus the underlying data. I find that breaches do not significantly affect hospital fundamentals post-breach, except through increases in fixed assets, which is consistent with Choi et al. (2020). There is no incremental effect for hacks.

Why might investors not require an incremental premium for investing in bonds issued by a hacked hospital when only hacks threaten hospital cash flows? Investors may be limited in their information regarding the differences between hacks and non-hacks. Municipal bond investors, primarily retail investors, are likely uninformed regarding the nuances of cyber risk and apply equal weight to any cyber event reported under HIPAA (Ablan et al., 2016; Mayer et al., 2021; MSRB, 2022). Alternatively, investors may be responding to changes in patient outcomes, which could adversely affect future hospital cash flows if providers prolong periods of lesser care. The evidence thus far points more towards the former explanation, but I rule out the alternative in later tests that examine patient outcomes.³⁸

3.3.4. Patient Health

I next examine whether investors require premiums for breached hospital bonds because of how data breaches affect patient care. Hypothetically, if data breaches adversely impact patient care, then patients should provide negative reports about their care and have worse outcomes than the patients of non-breached providers. Hacked hospitals should have the worst outcomes. To test these hypotheses, I utilize a similar triple-differences framework with the same hospital-level controls as before. I include hospital-event and year-event fixed effects to parallel my bond-level tests (Baker et al., 2023). However, I further restrict my sample of data breaches

³⁸ Empirical research and anecdotal evidence are unclear regarding the term structure of cyber risk (Cavusoglu et al., 2004; Huang and Wang, 2021; Kamiya et al., 2021; Brooks, 2022; Crosignani et al., 2023; Osborne, 2023). In Appendices H and I, I examine if investors view cyber risk as more of a short-term or long-term risk for hospital performance. The hospital bond market provides a unique setting to contribute to this debate by providing an opportunity to evaluate how significant information asymmetry of underlying issuer health affects investor expectations of cyber risk over different time horizons. Using a stacked triple differences methodology, I find that the market does not require any differential premia over short-term bonds when investing in assets associated with mid- or long-term maturities. Investors seem uncertain regarding how cyber risk will influence issuers within any given horizon, contrasting risks that exist in only one subset of bonds, such as climate risk (Painter, 2022). Investors weigh the immediate repercussions of a breach with as much importance as they do the longer-term effects of the breach, but there is too much uncertainty to know when the effects will culminate. Investors may discount their uncertainty into bonds of all maturities, or they may not be fully informed about breaches and treat all events the same (Ablan et al., 2016; Mayer et al., 2021).

to include only those between the years of 2017 and 2018, due to data constraints from CMS's patient survey data, to ensure that I have a balanced panel of pre- and post-breach outcomes. I also limit my control group to non-treated hospitals in the same county as breached hospitals to minimize the influence of any unobserved socio-economic factors that may influence the average patient to pursue or receive healthcare (McLaughlin and Wyszewianski, 2002; Kolossvary et al., 2023).

Like Aghamolla et al. (2023), I measure the patient care experience by first using patient survey data with seven proxies. The seven dependent variables I use are *Recommend "Yes"*, *Room Always Clean*, *Doc Comm Always Clear*, *Nurse Comm Always Clear*, *Recovery Info Always Clear*, *Room Always Quiet*, and *Rate "9-10"*. The variables are the percentage of patients who positively affirm their hospital's level of care in each of the respective categories. I present the results of my analysis of survey results in **Table 15**. I find that there is no association between data breaches and how patients rate their hospital care experience. Patients of treated hospitals report no differences in their quality of care across any dimension post-breach than patients of the same hospital before a breach.

However, patient survey data can be skewed by a plethora of unmeasurable factors. To mediate this concern and address whether patient care quantitatively changes post-breach, I employ 30-day readmission rate data from CMS for four of the most frequent ailments of emergency department patients. The diagnoses include pneumonia (*PN*), heart failure (*HF*), heart attack (acute myocardial infarction, *AMI*), and chronic obstructive pulmonary disease (*COPD*). If hospitals' level of care suffers because of breaches, then their readmission rates should increase, indicating that care providers were unable to properly treat the underlying ailment during a

patient's first visit (Jencks et al., 2009). Following Aghamolla et al. (2023), I examine both the level and log-transformed hospital readmission rates in **Table 16**.

Table 16 presents results based on my main sample specification with the control hospitals being all non-breached hospitals in the same county as a breached entity. I find exactly the opposite effect of what would be expected given the results in **Table 13**. I find that the 30-day readmission rates for pneumonia, heart attacks, and COPD decrease on average 14.4%, 30.2, and 29.2% after a data breach, respectively. Additionally, hacked hospitals experience economically meaningful increases in their readmissions for each condition when compared to the outcomes of non-breached hospitals within the same county, implying that hacks lead to subpar quality of care. Under the traditional interpretation of these results, it would seem that care improves, on average, after a hospital reports a data breach but incrementally worsens if a breach is a hack. The medical literature suggests that an average improvement in care is potentially attributable to mandatory staff training following a breach, while the worse performance after a hack is likely due to healthcare providers' inability to effectively access systems or equipment used in the modern healthcare environment (Forsetlund et al., 2021; Dameff et al., 2023; GHP, 2023).

Changes in patient care do not fully explain investors' response to data breaches, especially since they do not respond to the worst types of events. Investors may require greater premiums for breached hospital bonds out of concern that breaches will lead to worse hospital performance, but their reservations are seemingly misplaced. Only hacks harm hospital financial health and patient health.

3.4. The Role of Attention

Lastly, I identify how attention to data breach news affects information asymmetry surrounding hospital data breaches. If attention mitigates information asymmetry around breaches, my previous results should be weaker when attention on data breaches is greater. Alternatively, attention could accentuate misinformation and information asymmetry. Motivated by Da et al. (2011), I use Google Trends SVI of news articles that include the phrase “data breach” to proxy for attention around hospital data breaches. I base my collection of SVI on news articles to better account for both the release of information related to cyber risk and potential stakeholder attention to data breaches, but my results are qualitatively similar if base SVI on standard web search queries. I collect SVI at the state-level for each issuer and hospital for a seven-year window surrounding their breaches, average the SVI to the yearly-level for each state-event, and identify whether an observation is associated with a high (low) SVI. I assume that SVI is high (low) if it is greater (lower) than the median SVI for the overall sample.

I repeat both the hospital cash flow and financing tests of Tables 14 and 12 in Panels A and B of **Table 17**, respectively, for periods of high and low attention. I find that the effects of data breaches are much greater when there is more attention on data breaches. For example, the effect of hacks on total patient revenue in high-SVI periods is over twice as large as the effect in low-SVI periods. In contrast, hospital financing costs increase almost exclusively in high-SVI periods. These results imply that hacks harm hospital health no matter when they occur, but investors do not penalize issuers unless there is already elevated attention on similar events.

Given the evidence presented by Ablan et al. (2016) and Mayer et al. (2021), it is likely safe to assume that municipal bond market investors do not fully understand the differences between hacks and non-hacks, thereby explaining why investors do not appropriately price the

worst events. Yet, the results presented in **Table 17** show that municipal bond investors are further influenced by the prevailing level of attention on data security and, consequently, fail to incorporate relevant information into the assets' prices.

4. Robustness Tests

In this section, I briefly address three potential concerns with my methodology. The first concern centers on the robustness of the stacked difference-in-differences methodology. The second and third concerns pertain to my construction of counterfactual observations. I address each criticism by reproducing the main results from **Table 12** using alternative econometric or sample specifications.

4.1. Alternative Approach to Dealing with Heterogeneous Treatment Effects

The first criticism I address focuses on limitations potentially imposed by the stacked difference-in-differences estimator. Although the model is designed to be robust to heterogeneous treatment effects over a sample period, the stacked difference-in-differences estimator may be considered less flexible than other alternatives to the staggered difference-in-differences estimator (Baker et al., 2022). As such, I ensure robustness to the methodology proposed by Borusyak et al. (2023) and use a similar set of control variables to my main specification and control bonds from never treated issuers over the entire sample period.

I present the results in Panel A of **Table 18** and find that my main results hold. Models 1-4 all produce coefficients of the ATT that are both statistically significant and similar in magnitude to those produced by the stacked difference-in-differences estimator. According to the imputation estimator proposed by Borusyak et al. (2023), data breaches increase the new offer yields of breached hospitals by almost 12.8% and tax-adjusted spreads by about 26.6% relative to the mean of each variable, respectively.

4.2. Sample Construction and Alternative Counterfactuals

It could be that my results are driven by my sample construction choices. As such, I employ two alternative approaches to constructing my controls.

First, I identify control observations by matching treated bonds to control observations on bond characteristics using coarsened exact matching. This approach may help difference out the effect that any observable bond characteristic may have on the outcome and may control for any systemic differences between treated and non-treated issuers. I match each treated bond to a control bond issued within the same year and that has the same categorical characteristics (i.e., callable, negotiated, etc.). I split the continuous bond-level control variables from **Table 12**, county population, and county employment into four bins and further match the treated observations to the control observations within the same bin. I repeat my main analysis using the coarsened exact matched sample in Panel B of **Table 18**. Although the matched sample produces estimates of the ATT that are larger than the baseline coefficients in **Table 12** without control variables, the coefficients are similar in magnitude when the models are estimated with control variables.

Second, instead of using all non-breached issuers within a state as controls, I use only non-breached neighboring issuers within the same county. This difference in the construction of the control group may better account for the influence of any unobserved factors, such as geography or demographic differences that may be associated with a population's response to a breach, on the cost of hospital financing. If breaches truly affect hospital financing and societal outcomes, then the effect should exist when contrasting breached issuers with their geographical neighbors. I present the results of my second alternative approach to constructing the counterfactuals in Panel C of **Table 18**. The sample size decreases to a total of 2.8k bonds, but

the main results still hold. The estimated coefficients are larger than those presented in **Table 12** but are more comparable to those presented in **Table 13**. Furthermore, the results are largely in line with both those presented in **Table 12** and the other robustness tests.

5. Conclusion

Although cyberattacks and data breaches are known to be costly events for victims, little is known about how the events affect stakeholders of breached entities. Likewise, most of the extant empirical research assumes that market participants know both the extent and nature of data breaches when examining how they affect real and financial outcomes. Because of the strict medical data breach reporting requirements but delayed reporting of hospital finances, the hospital bond market provides a unique opportunity to identify how data breaches affect non-breached stakeholders and how information asymmetry about data breaches influences the stakeholder response.

Using the near universe of medical data breaches, this paper is the first to examine how data breaches affect hospital financing and patient outcomes. I find that breaches increase the cost of hospital bonds and are associated with increases in a hospital's credit and cash flow risk. I further find that hacks are the most adverse type of breach for hospitals, but investors do not incrementally respond to hacks relative to the average breach. In other words, investors misprice healthcare bonds by penalizing the wrong group of breached issuers. Investors appear indifferent regarding the nuances of different types of breaches and are further influenced by the prevailing levels of attention on data breaches.

My study has important implications for researchers, policymakers, and patients. First, my bond-level results imply that investors may not fully grasp the importance or relevance of different types of data breaches and how the events affect underlying cash flows. This lack of

understanding leads some hospitals to pay more for their debt than they likely should. Second, my hospital-level results imply that hacks have adverse consequences for local hospitals. The medical literature shows that such events could easily lead to crisis-level scenarios where healthcare providers are unable to properly serve their patients (Burky, 2023; Dameff et al., 2023). To alleviate these concerns, policymakers could require stronger IT standards for hospitals to minimize the number of hacks from occurring. Additionally, policymakers could implement regulations and programs that aid hospitals' post-hack recovery, increase investor awareness of cyber risk, or implement programs to quickly restore public trust in breached hospitals.

References

- Ablan, L., P. Heaton, D. Lavery, and S. Romanosky, 2016, Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information, *RAND Corporation*, Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.
- Aghamolla, C., P. Karaca-Mandic, X. Li, and R. Thakor, 2023, Merchants of Death: The Effect of Credit Supply Shocks on Hospital Outcomes, *NBER Working Paper* 28709.
- Akey, P., S. Lewellen, I. Liskovich, and C. Schiller, 2021, Hacking Corporate Reputations, Available at SSRN 3143740.
- American Hospital Association (AHA), 2022, Fact Sheet: Economic Contribution of Hospitals, Available at: [https://www.aha.org/fact-sheets/2022-02-25-fact-sheet-economic-contribution-hospitals#:~:text=When%20you%20add%20in%20these,U.S.%20\(see%20Figure%202\)](https://www.aha.org/fact-sheets/2022-02-25-fact-sheet-economic-contribution-hospitals#:~:text=When%20you%20add%20in%20these,U.S.%20(see%20Figure%202).).
- Amir, E., S. Levi, and T. Livne, 2018, Do Firms Underreport Information on Cyber-attacks? Evidence from Capital Markets, *Review of Accounting Studies* 23, 1177-1206.
- Andreadis, L., E. Kalotychou, C. Louca, C. Lundblad, and C. Makridis, 2023, Cyberattacks, Media Coverage, and Municipal Finance, Available at SSRN 4473545.
- Ashraf, M., 2022, The Role of Peer Events in Corporate Governance: Evidence from Data Breaches, *The Accounting Review* 97, 1-24
- Baker, A., D. Larker, and C. Wang, 2022, How Much Should We Trust Staggered Difference-in-Differences Estimates?, *Journal of Financial Economics* 144, 370-395.
- Borusyak, K., X. Jaravel, and J. Spiess, 2022, Revisiting Event Study Designs: Robust and Efficient Estimation, Available at SSRN 2826228.

- Brooks, C., 2022, Alarming Cyber Statistics for Mid-Year 2022 that You Need to Know, *Forbes*, July 3, 2022.
- Burky, A., 2023, Scripps Ransomware Post-Mortem Reveals Significant Ripple Effects for Nearby Hospitals, *FierceHealthCare.com*, Available at: <https://www.fiercehealthcare.com/health-tech/scripps-ransomware-post-mortem-shows-cybersecurity-regional-problem>.
- Butler, A., L. Fauver, and S. Motal, 2009, Corruption, Political Connections, and Municipal Finance, *Review of Financial Studies* 22, 2873-2905.
- Cabazon, F., 20203, The Effect of Mandatory Information Disclosure on Financial Constraints, *SSRN Working Paper* 3725099.
- Callaway, B. and P. Sant'Anna, 2021, Difference-in-Differences with Multiple Time Periods, *Journal of Econometrics* 225, 200-230.
- Calvert, S. and J. Kamp, 2019, Cyberattack Hobbles Baltimore for Two Weeks and Counting, *The Wall Street Journal*, May 29, 2019.
- Calvert, S. and J. Kamp, 2019, Hackers Won't Let Up in Their Attack on U.S. Cities, *The Wall Street Journal*, June 7, 2019.
- Campbell, K., L. Gordon, M. Loeb, and L. Zhou, 2003, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security* 11, 431-448.
- Cavusoglu, H., B. Mishra, and S. Raghunathan, 2004, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce* 9, 69-104.

- Cengiz, D., A. Dube, A. Lindner, and B. Zipperer, 2019, The Effect of Minimum Wages on Low-Wage Jobs, *Quarterly Journal of Economics* 134, 1405-1454.
- Centers for Disease Control and Prevention (CDC), 2020, QuickStats: Percentage of Deaths, by Place of Death – National Vital Statistics System, United States, 2000-2018, *Morbidity and Mortality Weekly Report* 69, 611.
- Cestau, D., B. Hollifield, D. Li, and N. Schürhoff, 2019, Municipal Bond Markets, *Annual Review of Financial Economics* 11, 65-84.
- Cheng, X. and S. Walton, 2019, Do Nonprofessional Investors Care about How Data Breaches are Disclosed, *Journal of Information Systems* 33, 163-182.
- Choi, S., M. E. Johnson, and J. Lee, 2020, An Event Study of Data Breaches and Hospital IT Spending, *Health Policy and Technology* 9, 372-378.
- Christensen, H., E. Floyd, L. Liu, and M. Maffett, 2017, The Real Effects of Mandated Information on Social Responsibility in Financial Reports: Evidence from Mine-Safety Records, *Journal of Accounting and Economics* 64, 284-304.
- CISA, 2021, Defending Against Software Supply Chain Attacks, *Cybersecurity and Infrastructure Security Agency*.
- Cornaggia, J., K. Cornaggia, and R. Israelsen, 2018, Credit Ratings and the Cost of Municipal Financing, *Review of Financial Studies* 31, 2038–2079.
- Cornaggia, K., X. Li, and Z. Ye, 2022, Virtual Competition and the Cost of Capital: Evidence from Telehealth, *Working Paper*.
- Cornaggia, K., J. Hund, G. Nguyen, and Z. Ye, 2022, Opioid Crisis Effects on Municipal Finance, *Review of Financial Studies* 35, 2019-2066.

- Croignani, M., M. Macchiavelli, and A. Silva, 2023, Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, *Journal of Financial Economics* 147, 432-448.
- Curti, F., I. Ivanov, M. Macchiavelli, and T. Zimmermann, 2023, City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity, *Available at SSRN 4465071*.
- Da, Z., J. Engelberg, and P. Gao, 2011, In Search of Attention, *Journal of Finance* 66, 1461-1499.
- Dameff, C., J. Tully, T. Chan, E. Castillo, S. Savage, T. Hemmen, B. Clay, and C. Longhurst, 2023; Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the US, *JAMA Network Open* 6, e2312270.
- Fenna, M., 2022, Cyber-attacks Are Inevitable: Prioritise Data Skills Training to Reduce Risk, *TrainingZone*.
- Florakis, C., C. Louca, R. Michaely, and M. Weber, 2023, Cybersecurity Risk, *Review of Financial Studies* 36, 351-407.
- Forsetlund, L., M. O'Brien, L. Forsen, L. Mwai, L. Reinart, M. Okwen, T. Horsley, and C. Rose, 2021, Continuing Education Meetings and Workshops: Effects on Professional Practice and Healthcare Outcomes, *Cochrane Database Systems Review* 9, CD003030.
- Gao, P. C. Lee, and D. Murphy, 2020, Financing Dies in Darkness? The Impact of Newspaper Closures on Public Finance, *Journal of Financial Economics* 135:445-467.
- Gao, H. and W. Zhang, 2017, Employment Nondiscrimination Acts and Corporate Innovation, *Management Science* 63:2982-2999.
- GHP News, 2023, How Hospital Security Improves Patient Satisfaction, *GHP News*, Available at: <https://ghpnews.digital/how-hospital-security-improves-patient-satisfaction/>.

- Griffin, P., 2003, Got Information? Investor Response to Form 10-K and Form 10-Q EDGAR Filings, *Review of Accounting Studies* 8, 433-460.
- Grigoris, F., 2020, The Term Structure of Municipal Bond Yields, Local Economic Conditions, and Local Stock Returns, PhD Thesis, The University of North Carolina at Chapel Hill.
- Gustafson, M., P. Haslag, D. Weagley, and Z. Ye, 2023, A Flash in the Pan(demic)? Migration Risks and Municipal Bonds, *Available at SSRN 4029984*.
- Gundersen, C., B. Kreider, and J. Pepper, 2011, The Economics of Food Insecurity in the United States, *Applied Economic Perspectives and Policy* 33, 281-303.
- Hovav, A., and J. D’Arcy, 2003, The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms, *Risk Management and Insurance Review* 6, 97-121.
- Huang, H., and C. Wang, 2021, Do Banks Price Firms’ Data Breaches?, *The Accounting Review* 96, 261-286.
- Jackson, C., C. Wigger, and H. Xiong, 2021, Do School Spending Cuts Matter? Evidence from the Great Recession, *American Economic Journal: Economic Policy* 13, 304-335.
- Jamilov, R., H. Rey, and A. Tahoun, 2021, The Anatomy of Cyber Risk, *NBER Working Paper* 28906.
- Jencks, S. F., M. V. Williams, and E. A. Coleman, 2009, Rehospitalizations among Patients in the Medicare Fee-for-Service Program, *New England Journal of Medicine* 360, 1418-1428.
- Jensen, J. and F. Paine, 2023, Municipal Cyber Risk, *Working Paper*.
- Jerch, R., M. Kahn, and G. Lin, 2023, Local Public Finance Dynamics and Hurricane Shocks, *Journal of Urban Economics* 134, 103516.

- Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz, 2021, Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms, *Journal of Financial Economics* 139, 719-749.
- Kannan, K., J. Rees, and S. Sridhar, 2007, Market Reactions to Information Security Breach Announcements: An Empirical Analysis, *International Journal of Electronic Commerce* 12, 69-91.
- Kashyap, A. K. and A. Wetherilt, 2019, Some Principles for Regulating Cyber Risk. *AEA Papers and Proceedings* 109, 482-487.
- Kolossvary, E., K. Farkas, O. Karahan, J. Golledge, G. Schernthaner, T. Karplus, J. Bernardo, S. Marschang, M. Abola, M. Heinzmann, M. Edmonds, and M. Catalano, 2023, The Importance of Socio-Economic Determinants of Health in the Care of Patients with Peripheral Artery Disease: A Narrative Review from VAS, *Vascular Medicine* 28, 241-253.
- Kvochko, E., and R. Pant, 2015, Why Data Breaches Don't Hurt Stock Prices, *Harvard Business Review*.
- Lerman, A. and J. Livnat, 2009, The New Form 8-K Disclosures, *Review of Accounting Studies* 15, 752-778.
- Lin, Z., T. Sapp, J. Ulmer, and R. Parsa, 2020, Insider Trading Ahead of Cyber Breach Announcements, *Journal of Financial Markets* 50, 100527.
- MacDorman, M. and E. Declercq, 2019, Trends and State Variations in Out-of-Hospital Births in the United States, 2004-2017, *Birth* 46, 279-288.
- Mayer, P., Y. Zou, F. Schaub, and A. Aviv, 2021, "Now I'm a Bit Angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them, *30th USENIX Security Symposium*.

- McLaughlin, C. and L. Wyszewianski, 2002, Access to Care: Remembering Old Lessons, *Health Services Research* 37, 1441-1443.
- Municipal Rulemaking Securities Board (MSRB), 2022, Trends in Municipal Securities Ownership.
- Muolo, D., 2022, Cybersecurity Investments Could Go by the Wayside at Cash-Strapped Hospitals, Fitch Warns, FierceHealthcare.com, Available at: <https://www.fiercehealthcare.com/providers/cybersecurity-preparations-could-go-wayside-cash-strapped-hospitals-fitch-warns>.
- Osborne, B., 2023, When Government Catches the (Cyber) Bug: The Costs and Real Effects of Municipal Cyberattacks, *Working Paper*.
- Painter, M., 2022, An Inconvenient Cost: The Effects of Climate Change on Municipal Bonds, *Journal of Financial Economics* 135, 468-482.
- Pierson, K., M. Hand, and F. Thompson, 2015, The Government Finance Database: A Common Resource for Quantitative Research in Public Financial Analysis, *PLoS ONE* 10:e0130119.
- Rizzi, C., 2023, Nature as a Defense from Disasters: Natural Capital and Municipal Bond Yields, *Available at SSRN* 4038371.
- Securities and Exchange Commission (SEC), 2011, CF disclosure guidance: Topic No. 2: Cybersecurity, Available at: <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.
- Securities and Exchange Commission (SEC), 2018, Commission statement and guidance on public company cybersecurity disclosures, Available at: <https://www.sec.gov/rules/interp/2018/33-10459.pdf>

- Serfling, M., 2016, Firing Costs and Capital Structure Decisions, *Journal of Finance* 71, 2239-2285.
- Shandler, R. and M. Gomez, 2023, The Hidden Threat of Cyber Attacks – Undermining Public Confidence in Government, *Journal of Information Technology & Politics* 20, 359-374.
- Tanimura, J. and E. Wehrly, 2015, The Market Value and Reputational Effects from Lost Confidential Information, *International Journal of Financial Management* 5, 18-35.
- Tosun, O., 2021, Cyber-attacks and Stock Market Activity, *International Review of Financial Analysis* 76.
- Tran, N. and C. Uzmanoglu, 2022, COVID-19, Lockdowns, and the Municipal Bond Market, *Journal of Banking and Finance* 106590.
- Vakili, K. and L. Zhang, 2018, High on Creativity: The Impact of Social Liberalization Policies on Innovation, *Strategic Management Journal* 39, 1860-1886.

Appendix

Appendix A Targeted Counties

This table presents the targeted counties I include in my primary sample. All bonds issued by these counties are associated with the variable *Target* that equals one, and the variable *Target* equals zero for all bonds issued by other non-targeted counties in the same state in my later analysis. The *Date Made Public* and *Source* columns represent the announcement date and associated sources recorded by the PRC database.

Date Made Public	County	State	Source
7/29/2005	San Diego	California	Dataloss DB
7/26/2006	Los Angeles	California	Dataloss DB
5/31/2007	Fresno	California	Dataloss DB
12/20/2007	Franklin	Ohio	Dataloss DB
9/30/2008	Jefferson	Colorado	Dataloss DB
10/21/2011	Baldwin	Alabama	Databreaches.net
12/15/2011	Montgomery	Pennsylvania	Databreaches.net
1/31/2012	Greene	Ohio	Dataloss DB
2/27/2012	Los Angeles	California	Databreaches.net
4/14/2012	Berrien	Michigan	Dataloss DB
4/26/2012	Hennepin	Minnesota	Dataloss DB
5/6/2012	Lake	Florida	Databreaches.net
5/13/2012	York	South Carolina	Dataloss DB
8/14/2013	Harris	Texas	Media
10/10/2013	Monterey	California	Media
1/13/2014	King	Washington	Media
12/15/2016	Los Angeles	California	California AG

Appendix B

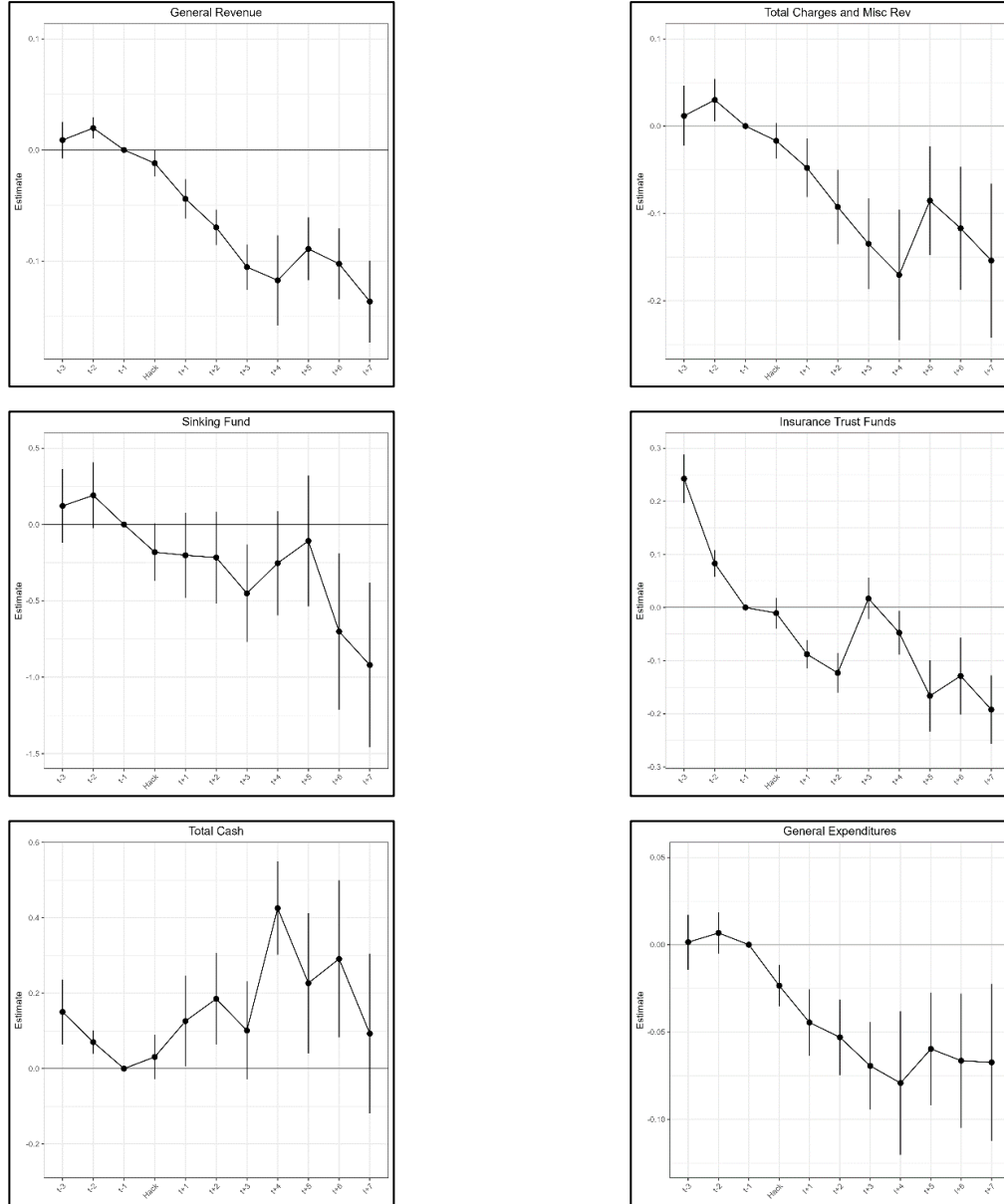
Variable Definitions for Chapter 1

This table provides the definitions for the main variables used in this study. Variables denominated in dollars are inflation-adjusted to 2009 dollars.

Variable	Definition
<i>Adjusted Spread</i>	<i>Spread</i> adjusted by the highest state-level marginal tax rate for each year in my sample
<i>Amount</i>	The bond issue amount
<i>Callable</i>	An indicator that equals 1 if a bond is callable, 0 otherwise
<i>Coupon</i>	A bond's coupon amount from SDC
<i>Employment</i>	The county employment level from the BEA's CAIN30 dataset
<i>General Expenditures</i>	County-level general expenses from Pierson et al. (2015)
<i>General Revenue</i>	County-level general revenue from Pierson et al. (2015)
<i>GO Bond</i>	An indicator that equals 1 if a bond is a general obligation bond
<i>Insurance Trust Funds</i>	County-level insurance funds held in trust from Pierson et al. (2015)
<i>Insured</i>	An indicator that equals 1 if a bond is insured, 0 otherwise
<i>Inverse Maturity</i>	One divided by <i>Maturity</i>
<i>Maturity</i>	The difference between a bond's maturity and settlement dates
<i>Max Rating</i>	A factor variable defined from 1 to 21 for the highest credit rating assigned to a bond; lower numbers are higher rated bonds
<i>Negotiated</i>	An indicator that equals 1 if a bond is negotiated, 0 otherwise
<i>Per Capita Income</i>	County-level per capita income from the BEA's CAIN30 dataset
<i>Population</i>	The county population level from the BEA's CAIN30 dataset
<i>Post</i>	An indicator that equals 1 if an observation is in a year after an attack, 0 otherwise
<i>Sinking Fund</i>	County-level funding set aside to pay off debt from Pierson et al. (2015)
<i>Spread</i>	<i>Yield</i> minus <i>Treasury Yield</i>
<i>Target</i>	An indicator that equals 1 if an observation is from a targeted county, 0 otherwise
<i>Tax Exempt</i>	An indicator that equals 1 if a bond is tax exempt, 0 otherwise
<i>Total Cash</i>	County-level cash and securities holding from Pierson et al. (2015)
<i>Total Charges and Misc Revs</i>	County-level charges and miscellaneous revenue from Pierson et al. (2015)
<i>Total Elementary Education Exp</i>	County-level elementary education expenses from Pierson et al. (2015)
<i>Total Health Exp</i>	County-level health-related expenditures from Pierson et al. (2015)
<i>Total Natural Resource Exp</i>	County-level natural resource project expenses from Pierson et al. (2015)
<i>Total Police Exp</i>	County-level police protection expenses from Pierson et al. (2015)
<i>Total Public Welfare Exp</i>	County-level welfare assistance from Pierson et al. (2015)
<i>Treasury Yield</i>	The maturity-matched yield on Treasury bonds, linearly interpolated for missing maturities
<i>Yield</i>	A bond's initial offer yield from SDC
<i>Urban</i>	An indicator that equals one if defined as Urban by the National Center for Health Statistics's 2013 Urban-Rural Classification Scheme

Appendix C

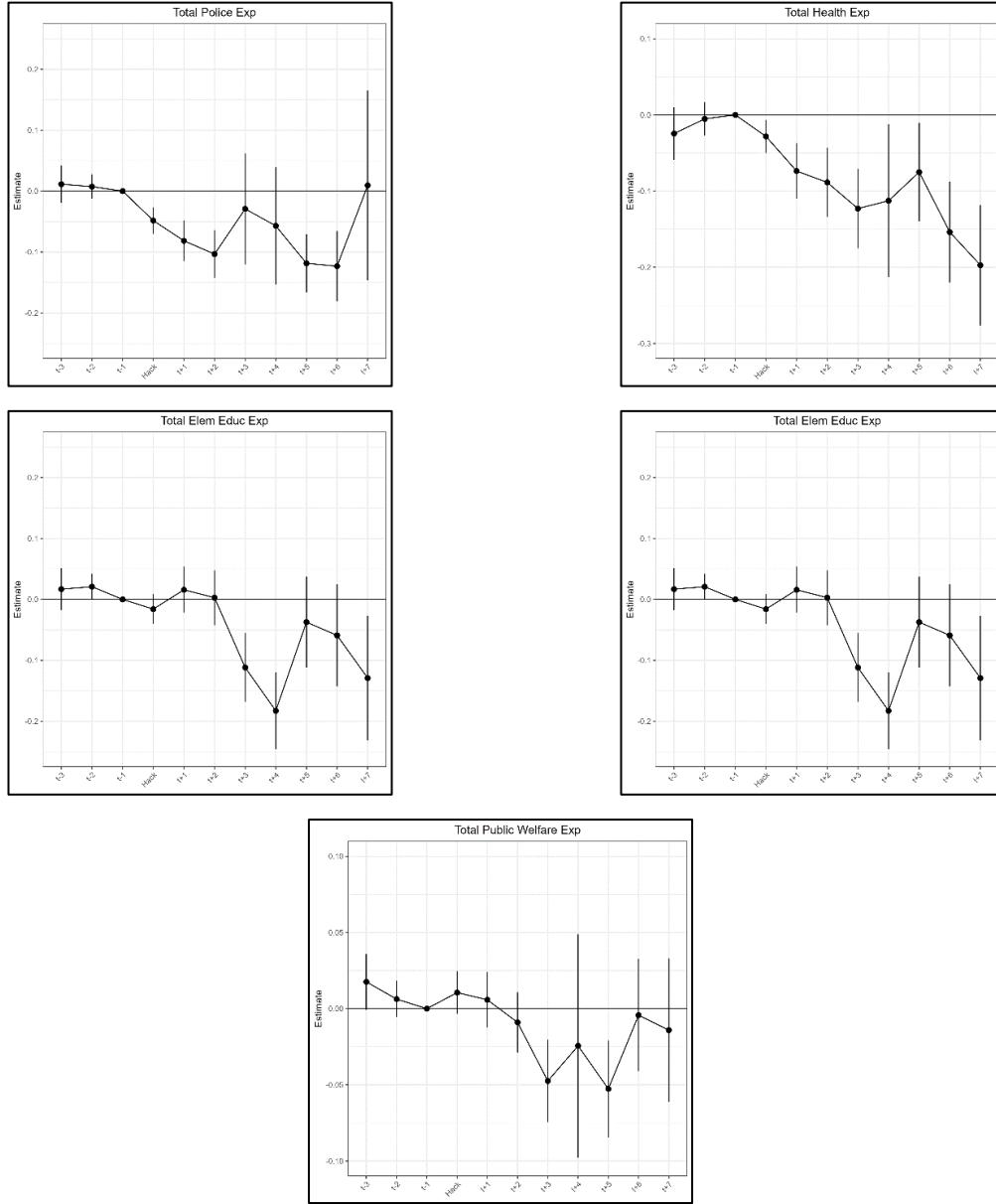
Timing of County Cash Flow Effects



This figure presents stacked difference-in-difference coefficient estimates of my county-level cash flow dependent variables on a set of timing variables interacted with *Target* estimated over the entire $[-7,7]$ window. The timing indicators are defined relative to the year of attack, where *Hack* is year t . However, I restrict the timing plots over the period $[-3,7]$ for easier viewing of the post-attack trends. I include county times event, year times event, and size decile times event fixed effects and the control variables *lag Population*, *lag Per Capita Income*, and *lag Employment* in each model. Following econometric tradition, I exclude the period $t-1$ in my estimation. The coefficients for the controls and level effects are omitted for brevity. The bars around the point estimates represent the 95% confidence intervals (Baker et al., 2022). All variables are defined in Appendix B.

Appendix D

Timing of County Social Spending Adjustment



This figure presents stacked difference-in-difference coefficient estimates of my county-level social spending dependent variables on a set of timing variables interacted with *Target* estimated over the entire $[-7,7]$ window. The timing indicators are defined relative to the year of attack, where *Hack* is year t . However, I restrict the timing plots over the period $[-3,7]$ for easier viewing of the post-attack trends. I include county times event, year times event, and size decile times event fixed effects and the control variables *lag Population*, *lag Per Capita Income*, and *lag Employment* in each model. Following econometric tradition, I exclude the period $t-1$ in my estimation. The coefficients for the controls and level effects are omitted for brevity. The bars around the point estimates represent the 95% confidence intervals (Baker et al., 2022). All variables are defined in Appendix B.

Appendix E

Variable Definitions for Chapter 2

This table provides the definitions for the main variables used in this study. Variables denominated in dollars are inflation-adjusted to 2009 dollars.

Variable	Definition
<i>Adjusted Spread</i>	<i>Yield</i> divided by 1 minus the highest state-level marginal tax rate for each year in my sample, less the corresponding <i>Treasury Yield</i>
<i>Always Clean</i>	The proportion of patients who report that their room was always clean
<i>Amount</i>	The bond issue amount
<i>Assets</i>	A hospital's total reported assets
<i>Bed Days</i>	A hospital's number of beds multiplied by the number of days in a year
<i>Bed Utilization</i>	A hospital's total number of discharges divided by <i>Bed Days</i>
<i>Breach</i>	An indicator that equals 1 if an observation is from a breached entity, 0 otherwise
<i>Callable</i>	An indicator that equals 1 if a bond is callable, 0 otherwise
<i>Cash</i>	A hospital's total cash in hand or in banks
<i>Coupon</i>	A bond's coupon amount from SDC
<i>Doctor Always Clear</i>	The proportion of patients who report their doctors always communicated clearly
<i>Employment</i>	The county employment level from the BEA's CAIN30 dataset
<i>Fixed Equipment</i>	A hospital's reported value of fixed assets
<i>GO Bond</i>	An indicator that equals 1 if a bond is a general obligation bond
<i>Hospital Income</i>	A hospital's total income
<i>Liabilities</i>	A hospital's total current and long-term liabilities
<i>Inpatient Revenue</i>	A hospital's revenue from inpatient services
<i>Inverse Maturity</i>	One divided by <i>Maturity</i>
<i>Maturity</i>	The difference between a bond's maturity and settlement dates
<i>Max Rating</i>	A factor variable defined from 1 to 21 for the highest credit rating assigned to a bond; lower numbers are higher rated bonds
<i>Negotiated</i>	An indicator that equals 1 if a bond is negotiated, 0 otherwise
<i>Nurse Always Clear</i>	The proportion of patients who report their nurses always communicated clearly
<i>Outpatient Revenue</i>	A hospital's revenue from outpatient services
<i>Per Capita Income</i>	County-level per capita income from the BEA's CAIN30 dataset
<i>Population</i>	The county population level from the BEA's CAIN30 dataset
<i>Post</i>	An indicator that equals 1 if an observation is in a year after an attack, 0 otherwise
<i>Rate "9-10"</i>	The proportion of patients who report they would rate a hospital a "9" or "10"
<i>Recommend "Yes"</i>	The proportion of patients who report they would recommend a hospital
<i>Recov Info Always Clear</i>	The proportion of patients who report their recovery information was always clear
<i>Room Always Quiet</i>	The proportion of patients who report their room was always quiet
<i>SVI</i>	The log of the yearly mean of the Google Trends score for the phrase "data breach" within a hospital's state
<i>Tax Exempt</i>	An indicator that equals 1 if a bond is tax exempt, 0 otherwise
<i>Treasury Yield</i>	The maturity-matched yield on Treasury bonds, linearly interpolated for missing maturities
<i>Yield</i>	A bond's initial offer yield from SDC

Appendix F

The Incremental Effect of External Hacks on Secondary Market Trades

This table presents stacked triple difference-in-difference coefficient estimates of *Weighted Yield* and *Adjusted Spread* on *Breach*, *Post*, and an interaction between *Breach* and *Post*. The variable *Weighted Yield* is the monthly dollar-weighted average yield of bond trades from the MSRB secondary market database. I examine trades within a seven-month window of a breach announcement. Models 2 and 4 include *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and trade month-event fixed effects in the models to parallel the levels of fixed effects used in Table 3 (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>			
	<i>Weighted Yield</i>		<i>Adjusted Spread</i>	
	(1)	(2)	(3)	(4)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	0.119 (0.642)	-0.044 (-0.178)	0.168 (0.581)	-0.592 (-1.24)
<i>Breach</i> × <i>Post</i>	0.384*** (5.04)	0.138* (1.80)	0.595*** (5.05)	0.436** (1.99)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Trade Month×Event FEs	Yes	Yes	Yes	Yes
Observations	15,560	15,560	15,560	15,560
<i>Adj R</i> ²	0.689	0.854	0.471	0.750

Appendix G

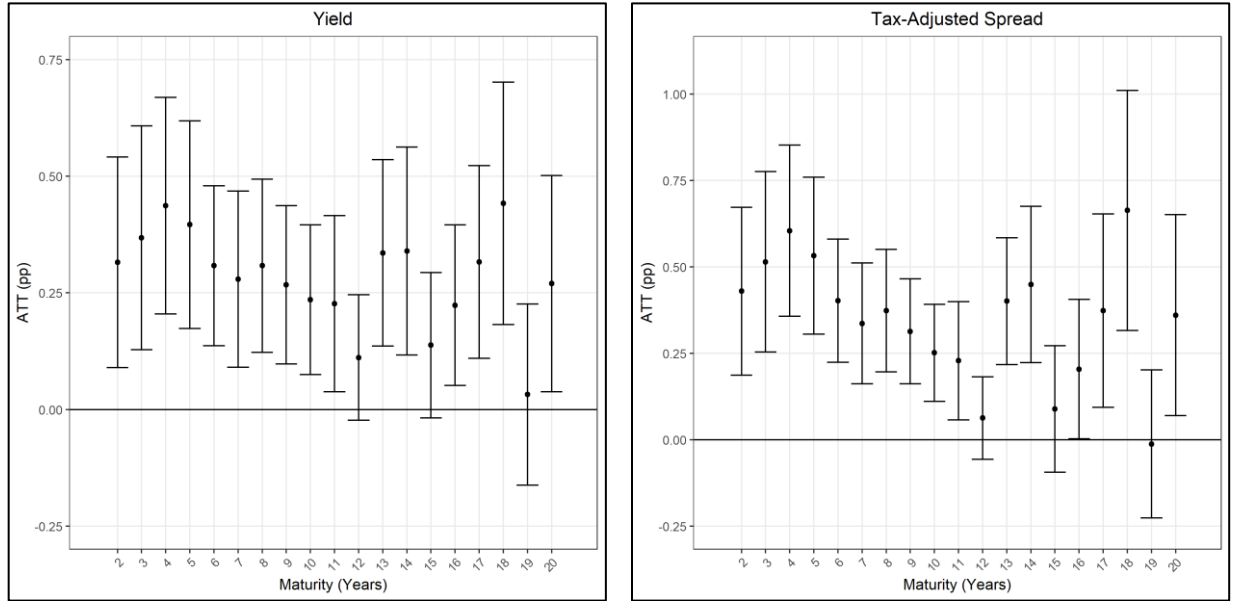
Fundamental Risk: Data Breaches and Hospital Health

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure hospital fundamental outcomes on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2015 and 2017 to ensure I have three years of pre- and post-breach outcomes. Each outcome is transformed by one plus the natural logarithm of the underlying variable. Each outcome variable is further scaled by the lagged total hospital revenue. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	logarithm of 1 + <i>Dependent Variable</i>			
	Assets/TR	Liabilities/TR	Cash/TR	Fixed Equipment/TR
	(1)	(2)	(3)	(4)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	-0.014 (-0.593)	-0.007 (-0.859)	0.0003 (0.234)	-0.058 (-1.492)
<i>Breach</i> × <i>Post</i>	0.005 (0.378)	0.009 (1.226)	0.001 (0.535)	0.008* (1.710)
Total Effect	-0.009	0.001	0.001	-0.049
<i>P</i> -Value	0.476	0.681	0.251	0.122
Controls	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	44,661	44,442	44,650	27,273
<i>Adj R</i> ²	0.956	0.973	0.997	0.907

Appendix H

Yield and Spread Curves of Treated Bonds



This figure presents the yield and spread curves of breached hospital bonds after a data breach for bonds that mature 2 to 25 years in the future. The point estimate for each maturity is based on a stacked difference-in-difference coefficient estimate of my two main dependent variables on a set of maturity timing variables interacted with *Breach*. I use the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The model estimating the yield curve includes the corresponding *Treasury Yield* as a control. The coefficients for the controls and level effects are omitted for brevity. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. I do not present the estimates for bonds with maturities longer than 25 years because there are few observations with maturities longer than 25 years. All variables are defined in Appendix E.

Appendix I

Term Structure of Breached Hospital Bonds

This table presents stacked difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, *Mid-Term*, *Long-Term*, and interactions between each of the terms. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Max Rating*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 1 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>	
	Yield (1)	Adjusted Spread (2)
<i>Breach</i> × <i>Post</i>	0.443* (1.94)	0.735** (2.20)
<i>Breach</i> × <i>Post</i> × <i>Mid-Term</i>	0.100 (0.455)	0.204 (0.712)
<i>Breach</i> × <i>Post</i> × <i>Long-Term</i>	-0.039 (-0.308)	-0.061 (-0.394)
Controls	Yes	Yes
Issuer×Event FEs	Yes	Yes
Year×Event FEs	Yes	Yes
Observations	11,987	11,987
<i>Adj R</i> ²	0.893	0.792

Figures

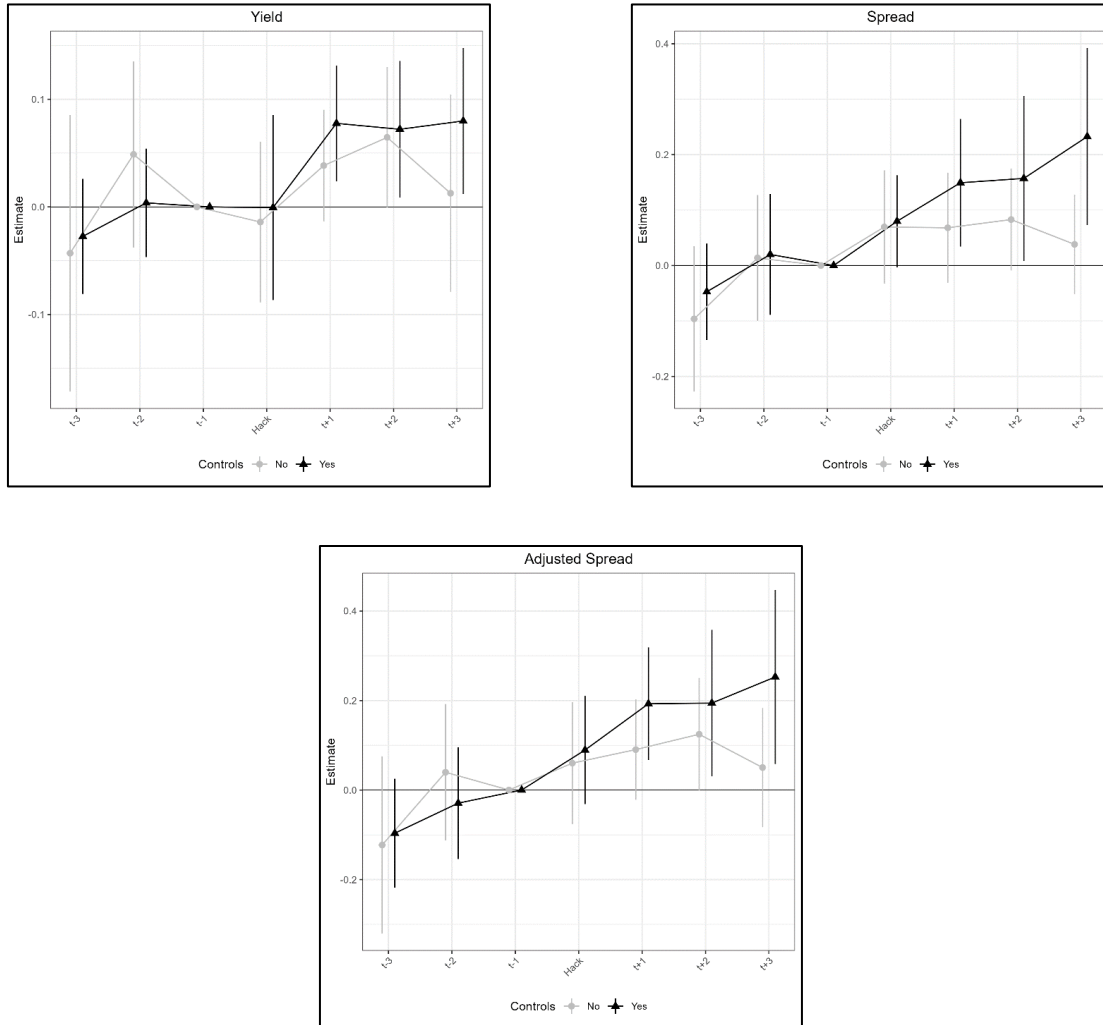


Figure 1. Analysis of Parallel Trends for County Bonds

This figure presents stacked difference-in-difference coefficient estimates of my three main dependent variables on a set of timing variables interacted with *Target*. The timing indicators are defined relative to the year of attack, where *Hack* is year t . Following econometric tradition, I exclude the period $t-1$ in my estimation. The models with control variables include *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The *Yield* model with controls also includes the corresponding *Treasury Yield* as a control variable. The coefficients for the controls and level effects are omitted for brevity. I include county-event and year-event fixed effects in each model, and the bars around the point estimates represent the 95% confidence intervals (Baker et al., 2022). All variables are defined in Appendix B.

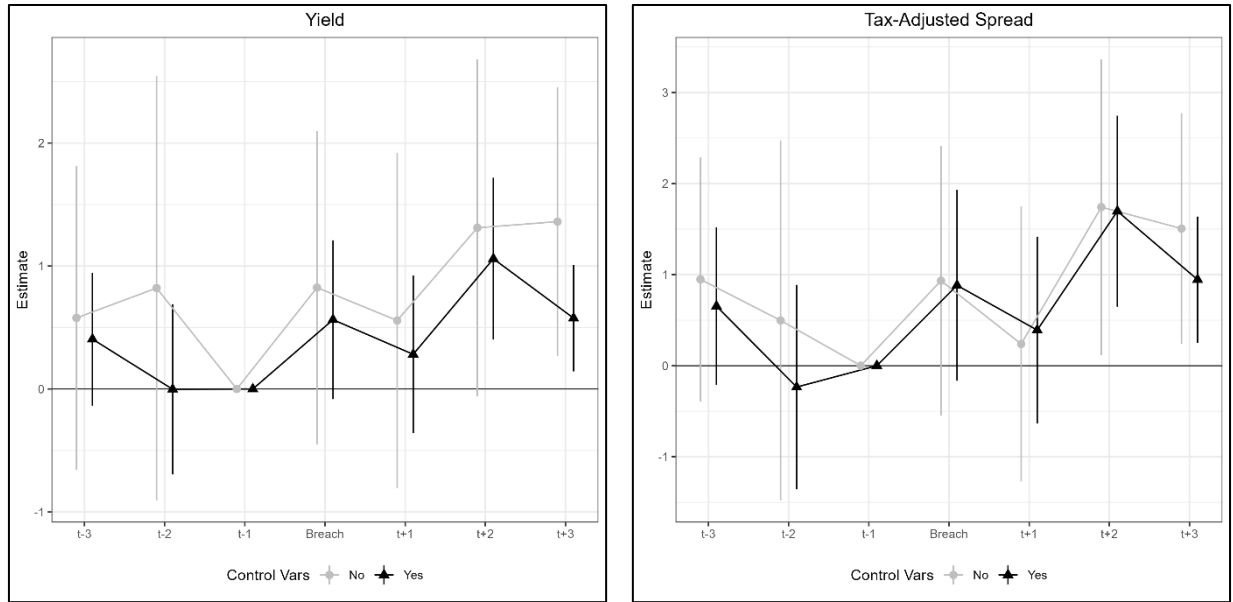


Figure 2. Timing of Healthcare Breach Effect

This figure presents stacked difference-in-difference coefficient estimates of my two main dependent variables on a set of timing variables interacted with *Breach*. The timing indicators are defined relative to the year of breach, where *Breach* is year t . Following econometric tradition, I exclude the period $t-1$ in my estimation. I use the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The model with *Yield* as a dependent variable includes the corresponding *Treasury Yield* as a control. The coefficients for the controls and level effects are omitted for brevity. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. All variables are defined in Appendix E.

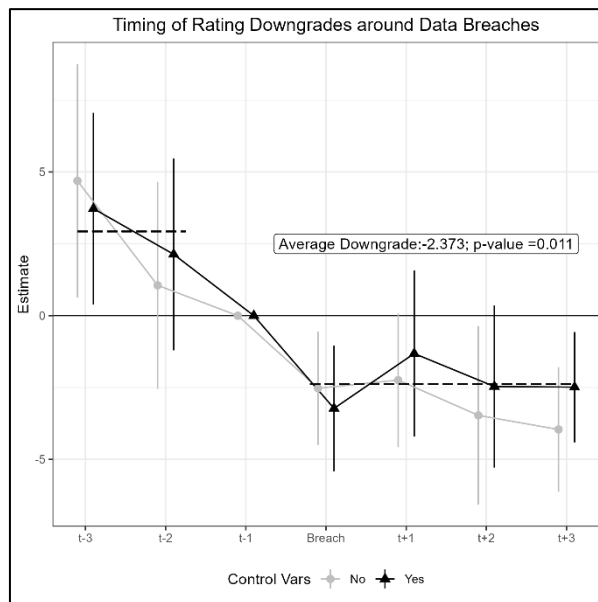


Figure 3. The Timing of Healthcare Bond Downgrades

This figure presents stacked difference-in-difference coefficient estimates of my max rating variables on a set of timing variables interacted with *Breach*. The timing indicators are defined relative to the year of breach, where *Breach* is year t . Following econometric tradition, I exclude the period $t-1$ in my estimation. I estimate one model without controls and one model with controls. I use the corresponding *Treasury Yield* and the variables *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. The coefficients for the controls and level effects are omitted for brevity. I compute the pre- and post-breach effect on bond ratings by averaging the two pre- (four post-) breach timing coefficients from the model with controls and testing the average's statistical significance using a Wald chi-squared test. I include issuer-event and year-event fixed effects in each model (Baker et al., 2022). Standard errors are clustered by issuer in all models, and the bars represent the 95% confidence interval. All variables are defined in Appendix E.

Tables

Table 1. Descriptive Statistics for Municipal Bonds and Counties

This table presents summary statistics for my main sample of municipal bonds issued by 17 targeted counties and their counterfactuals. Panel A presents statistics for my overall sample of bonds, and Panel B compares the treated and control samples of bonds. The last three rows in each panel represent county-level characteristics matched to municipal bonds and are in millions. Panel C presents statistics for my main sample of stacked county data. All continuous data are winsorized at the one percent level.

Panel A: Overall Sample of Bonds								
	N	Mean	SD	Pctl(25)	Median	Pctl(75)		
Yield (%)	444,368	3.09	1.31	2.13	3.18	4.04		
Spread (%)	280,074	1.16	0.95	0.45	0.94	1.60		
Adj Spread (%)	408,415	2.50	1.54	1.35	2.25	3.39		
Issue Size (MM)	444,368	80.89	150.02	8.97	26.17	80		
Bond Size (MM)	444,359	2.04	4.28	0.23	0.62	1.76		
Coupon (%)	444,368	3.85	1.12	3	4	5		
Maturity (Years)	444,368	10.23	6.7	4.88	9.21	14.53		
Max Rating	444,368	2.87	1.47	2	3	3		
GO	444,368	0.57	0.5	0	1	1		
Callable	444,368	0.91	0.28	1	1	1		
Insured	444,368	0.43	0.5	0	0	1		
Negotiated	444,368	0.76	0.42	1	1	1		
Tax Exempt	444,368	0.94	0.23	1	1	1		
Population _{t-1} (1,000s)	444,368	1,631.26	2,381.08	259	791	1,912		
Per Capita Income _{t-1} (1,000s)	444,368	44.10	14.72	33	41	51		
Employment _{t-1} (1,000s)	444,368	944.05	1,420.28	143	441	909		
Panel B: Treatment vs Control Samples of Bonds								
	Targeted				Non-Targeted			
	N	Mean	N	Mean	N	Mean	N	Mean
Yield (%)	58,656	2.97	3.01	1.27	385,712	3.11	3.2	1.31
Spread (%)	58,656	0.45	0.42	1.16	385,712	0.45	0.37	1.24
Adj Spread (%)	58,656	2.18	2.11	1.67	385,712	2.24	2.09	1.75
Issue Size (MM)	58,656	75.95	19.96	154.75	385,712	81.64	27.34	149.28
Bond Size (MM)	58,655	2.8	0.72	5.46	385,704	1.93	0.6	4.06
Coupon (%)	58,656	3.85	4	1.11	385,712	3.85	4	1.12
Maturity (Years)	58,656	10.24	9.26	6.62	385,712	10.23	9.21	6.71
Max Rating	58,656	3.01	3	1.55	385,712	2.85	3	1.46
GO	58,656	0.61	1	0.49	385,712	0.56	1	0.5
Callable	58,656	0.91	1	0.28	385,712	0.91	1	0.28
Insured	58,656	0.46	0	0.5	385,712	0.43	0	0.5
Negotiated	58,656	0.74	1	0.44	385,712	0.77	1	0.42
Tax Exempt	58,656	0.93	1	0.26	385,712	0.95	1	0.22
Population _{t-1} (1,000s)	58,656	6,301.02	4,557	3,639.13	385,712	921.12	684	835.07
Per Capita Income _{t-1} (1,000s)	58,656	47.99	49	9.18	385,712	43.50	40	15.30
Employment _{t-1} (1,000s)	58,656	3,820.86	3,104	2,035.15	385,712	506.57	325	494.12

Table 1
(Cont.)

Panel C: Overall Sample of Counties

	N	Mean	SD	Pctl(25)	Median	Pctl(75)
General Revenue (1,000s)	11,596	235,117.80	563,069.80	20,351.80	56,187.81	175,263.80
Total Charges and Misc Rev (1,000s)	11,596	77,188.21	163,197.80	8,385.17	20,057.68	64,355.22
Cash (1,000s)	11,596	295,573.60	879,340.80	9,467.39	33,009.71	153,640.60
Insurance Trust Funds (1,000s)	11,596	77,528.04	412,078.60	0	0	0
Sinking Funds (1,000s)	11,596	64,703.94	235,749.00	0	472.04	14,374.35
Total Elem Educ Exp (1,000s)	11,596	7,612.66	33,065.76	0	0	0
Total Health Exp (1,000s)	11,596	26,156.95	65,793.35	390.12	3,016.02	18,010.05
Total Public Welfare Exp (1,000s)	11,596	32,946.98	98,335.26	212.95	3,570.97	17,390.11
Total Police Prot Exp (1,000s)	11,596	17,557.81	41,131.93	1,777.48	4,422.43	13,383.64
Total Natural Resource Exp (1,000s)	11,596	2,736.34	8,763.20	0.88	244.21	1,164.75
General Exp (1,000s)	11,596	226,552.20	531,521.90	19,556.58	54,242.19	171,621.10
Population (1,000s)	11,596	204.08	376.45	25.51	67.48	201.17
Per Capita Income (1,000s)	11,364	37.41	12.21	29.36	35.41	42.77
Employment (1,000s)	11,364	129.34	355.2	11.8	32.56	107.91
Urban	11,596	0.39	0.49	0	0	1

Table 2. Determinants of Municipal Cyberattacks

This table analyzes which characteristics are associated with all county cyberattacks using a linear probability model. The dependent variable is a binary indicator that equals one if a county is attacked in a given year and zero otherwise, and all independent variables are transformed by the natural logarithm of one plus the underlying data. I estimate Models 1-3 with lagged independent variables. I estimate Models 4-6 with independent variables that are measured in changes over $t-1$ to t , but I exclude *Urban* as a control in Models 2-6 because the variable has no variation with the various levels of fixed effects or in a first difference specification. Standard errors are clustered by county in all models and presented in parentheses. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable: 1(Target_{i,t})</i>					
	Determinants Lagged			Differences in Logs from $t-1$ to t		
	(1)	(2)	(3)	(4)	(5)	(6)
Total Revenue	0.002 (0.001)	0.001 (0.001)	0.002* (0.001)	-0.006 (0.004)	-0.007 (0.004)	-0.006 (0.004)
Total Inc Tax	-0.0001 (0.0001)	-0.0001 (0.0001)	-0.0002 (0.0001)	-0.0001 (0.0001)	-0.0001 (0.0001)	-0.0001 (0.0001)
Total Cash	-0.0001 (0.0004)	-0.0002 (0.0003)	-0.0001 (0.0002)	-0.002 (0.001)	-0.002 (0.001)	-0.001 (0.001)
Population	0.002 (0.002)	0.004 (0.008)	0.004 (0.008)	0.065* (0.038)	-0.005 (0.067)	0.003 (0.056)
Per Capita Inc	0.005** (0.002)	0.001 (0.006)	0.002 (0.006)	0.005 (0.016)	0.011 (0.017)	0.005 (0.015)
Employment	-0.002 (0.002)	-0.010 (0.006)	-0.009* (0.005)	0.001 (0.012)	-0.008 (0.016)	-0.014 (0.015)
Urban	-0.001 (0.001)	-	-	-	-	-
State×Year FEs	Yes	Yes	No	Yes	Yes	No
County FEs	No	Yes	Yes	No	Yes	Yes
Year FEs	No	No	Yes	No	No	Yes
Observations	8,655	8,655	8,655	8,651	8,651	8,651
Adj R^2	0.005	-0.035	-0.036	0.003	-0.034	-0.035

Table 3. Impact of Cyberattacks on Cost of Municipal Debt

This table presents stacked difference-in-difference coefficient estimates of my three main dependent variables on *Target*, *Post*, and an interaction between *Target* and *Post*. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Models 1 and 2 also include the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include either state-event or county-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by county in all models and presented in parentheses. I drop all bonds with negative *Spread* and *Adjusted Spread* in Models 3-6. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>					
	Yield		Spread		Adjusted Spread	
	(1)	(2)	(3)	(4)	(5)	(6)
<i>Target</i> × <i>Post</i>	0.115*** (0.036)	0.050* (0.028)	0.165** (0.078)	0.126** (0.054)	0.230** (0.091)	0.178** (0.073)
<i>Target</i>	-0.032 (0.086)	-	-0.119 (0.150)	-	-0.133 (0.192)	-
Controls	Yes	Yes	Yes	Yes	Yes	Yes
State×Event FEs	Yes	No	Yes	No	Yes	No
County×Event FEs	No	Yes	No	Yes	No	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes
Observations	444,368	444,368	280,074	280,074	408,415	408,415
<i>Adj R</i> ²	0.785	0.799	0.425	0.484	0.608	0.642

Table 4. Term Structure of Cyber Risk

This table presents stacked difference-in-difference coefficient estimates of my three main dependent variables on *Target*, *Post*, and an interaction between *Target* and *Post* for three samples of bonds. The three samples involve short-term bonds (maturity less than 3 years), mid-term bonds (maturity between 3 and 10 years), and long-term bonds (maturity greater than 10 years). Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Models 1-3 also include the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in each model (Baker et al., 2022). The bottom row of the table tests whether the coefficient on *Target*×*Post* for the long sample is greater than the coefficient estimated for the short sample and presents both Z-statistics and p-values. I drop all bonds with negative *Spread* and *Adjusted Spread* in Models 4-9. All variables are defined in Appendix B. Standard errors are clustered by county in all models and presented in parentheses. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>								
	Yield			Spread			Adjusted Spread		
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
<i>Target</i> × <i>Post</i>	0.054 (0.053)	0.039 (0.038)	0.041* (0.023)	0.016 (0.026)	0.093 (0.057)	0.130* (0.066)	0.057 (0.051)	0.186** (0.080)	0.181** (0.091)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bond Sample	Short	Mid	Long	Short	Mid	Long	Short	Mid	Long
Observations	62,097	178,573	203,698	20,981	93,181	165,912	38,793	166,364	203,258
<i>Adj R</i> ²	0.692	0.763	0.763	0.412	0.389	0.537	0.383	0.500	0.643
$\beta_{Long} > \beta_{Short}$	Z = -0.575; p = 0.717			Z = 1.718; p = 0.043			Z = 1.360; p = 0.087		

Table 5. Municipal Bond Credit Risk and Issuances

This table compares stacked difference-in-difference coefficient estimates of *Max Rating* and the natural logarithm of *Total Issuance* on *Target*, *Post*, and an interaction between *Target* and *Post*. Model 1 includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *Tax Exempt*, the corresponding *Treasury Yield*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Because Model 2 is a county-level regression, it includes only *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. I do not include counties that have no issuance activity in Model 2. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in both models (Baker et al., 2022). Standard errors are clustered by county and presented in parentheses. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>	
	Max Rating	ln(Total Issuance)
	(1)	(2)
<i>Target</i> × <i>Post</i>	0.181** (0.073)	-0.061 (0.143)
Controls	Yes	Yes
County×Event FEs	Yes	Yes
Year×Event FEs	Yes	Yes
Observations	444,368	5,434
<i>Adj R</i> ²	0.357	0.775

Table 6. Investor Belief of Cash Flow Risk: General Obligation vs Revenue Bonds

This table compares stacked difference-in-difference coefficient estimates of my three main dependent variables on *Target*, *Post*, and an interaction between *Target* and *Post* across samples of general obligation (GO) and revenue (REV) bonds. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Models 1 and 2 also include the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in each model (Baker et al., 2022). The bottom row of the table tests whether the coefficient on *Target*×*Post* for the revenue bond sample is greater than the coefficient estimated for the general obligation bond sample and presents both Z-statistics and p-values. I drop all bonds with negative *Spread* and *Adjusted Spread* in Models 3-6. Standard errors are clustered by county and presented in parentheses. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>					
	Yield		Spread		Adjusted Spread	
	(1)	(2)	(3)	(4)	(5)	(6)
<i>Target</i> × <i>Post</i>	0.006 (0.034)	0.093*** (0.032)	0.061 (0.042)	0.204** (0.080)	0.069 (0.050)	0.267*** (0.096)
Controls	Yes	Yes	Yes	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes
Bond Sample	GO	REV	GO	REV	GO	REV
Observations	251,793	192,575	155,082	124,992	228,055	180,360
<i>Adj R</i> ²	0.823	0.773	0.511	0.501	0.670	0.647
$\beta_{Rev} > \beta_{GO}$	Z = 2.752; p = 0.003		Z = 1.790; p = 0.037		Z = 2.070; p = 0.019	

Table 7. Real Effects of Municipal Cyberattacks: Impact on County Cash Flows

This table examines the real impact of cyberattacks on several county-level outcomes that proxy for county cash flows. Each dependent variable is transformed by the natural logarithm, and I do not add one to the underlying data to ensure I compare only treated observations with relevant account data to counterfactuals with spending in the same account. I use a stacked difference-in-differences model over the window [-7,7] for calendar years 2001 to 2020 and require that counties have a full panel. The counterfactual observations are all non-targeted counties within the same state as the targeted county. Each model includes the variables *lag Population*, *lag Per Capita Income*, and *lag Employment* as controls. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in Panel A and add size decile-event fixed effects in Panel B to account for any size effect not accounted for with the control variables. Standard errors are clustered by county in all models and presented in parentheses. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	log(Dependent Variable)					
	General Revenue (1)	Total Charges and Misc Rev (2)	Sinking Fund (3)	Insurance Trust Funds (4)	Total Cash (5)	General Expenditures (6)
<i>Panel A: County×Event + Year×Event Fixed Effects</i>						
<i>Target×Post</i>	-0.100*** (0.013)	-0.105*** (0.031)	-0.422** (0.167)	-0.225*** (0.022)	0.055 (0.067)	-0.071*** (0.015)
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4,385	4,385	3,677	1,287	4,385	4,385
<i>Adj R²</i>	0.995	0.979	0.818	0.990	0.945	0.993
<i>Panel B: County×Event + Year×Event + Size Decile×Event Fixed Effects</i>						
<i>Target×Post</i>	-0.098*** (0.015)	-0.098*** (0.013)	-0.417** (0.189)	-0.208*** (0.020)	0.053 (0.072)	-0.070*** (0.016)
Controls	Yes	Yes	Yes	Yes	Yes	Yes
Observations	4,385	4,385	3,677	1,287	4,385	4,385
<i>Adj R²</i>	0.995	0.978	0.817	0.990	0.946	0.993

Table 8. Real Effects of Municipal Cyberattacks: Impact on County Reputation

This table examines the real impact of cyberattacks on several county-level outcomes that proxy for county cash flows. Each dependent variable is transformed by the natural logarithm, and I do not add one to the underlying data to ensure I compare only treated observations with relevant account data to counterfactuals with spending in the same account. I use a stacked difference-in-differences model over the window [-7,7] for calendar years 2001 to 2020 and require that counties have a full panel. The counterfactual observations are all non-targeted counties within the same state as the targeted county. Each model includes the variables *lag Population*, *lag Per Capita Income*, and *lag Employment* as controls. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in Panel A and add size decile-event fixed effects in Panel B to account for any size effect not accounted for with the control variables. Standard errors are clustered by county in all models and presented in parentheses. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	log(Dependent Variable)				
	Total Police Exp (1)	Total Health Exp (2)	Total Elem Educ Exp (3)	Total Natural Resource Exp (4)	Total Public Welf Exp (5)
<i>Panel A: County×Event + Year×Event Fixed Effects</i>					
<i>Target×Post</i>	-0.074** (0.031)	-0.124*** (0.027)	-0.080** (0.036)	-0.425*** (0.072)	-0.022 (0.016)
Controls	Yes	Yes	Yes	Yes	Yes
Observations	4,385	4,385	3,163	3,812	4,385
<i>Adj R²</i>	0.957	0.939	0.989	0.878	0.980
<i>Panel B: County×Event + Year×Event + Size Decile×Event Fixed Effects</i>					
<i>Target×Post</i>	-0.091*** (0.028)	-0.115*** (0.028)	-0.079** (0.039)	-0.399*** (0.080)	-0.033* (0.017)
Controls	Yes	Yes	Yes	Yes	Yes
Observations	4,385	4,385	3,163	3,812	4,385
<i>Adj R²</i>	0.959	0.942	0.990	0.879	0.980

Table 9. Robustness of County Financing Tests

This table presents robustness tests for my main results in Table 3. I use a stacked difference-in-difference estimation in each model, and the columns represent coefficient estimates of my three main dependent variables on *Target*, *Post*, and an interaction between *Target* and *Post*. Each model includes *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 1 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include county-event and year-event fixed effects in the models (Baker et al., 2022). Panel A addresses the generalizability of my results by including city bonds in the sample. Panel B excludes the last two hacks on Los Angeles. Panel C includes bonds with negative spreads and tax-adjusted spreads. Panel D only non-targeted, neighboring counties within the same state as controls. Panel E is based on a propensity score match using Model 1 from Table 2, except with the natural logarithm of the variables *Population*, *GDP per Capita*, and *Employment*, to identify controls within a 15% caliper and match control counties to targets in the same state and year. Panel F presents my main financing test models using an alternative methodology (Callaway and Sant’Anna, 2021) over the same sample period as my primary sample. Each model in Panel D includes *Coupon*, *Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 1 also includes the corresponding *Treasury Yield* as a control, but I exclude the variable *Inverse Maturity* as a control variable because it prevents the first stage of the Callaway and Sant’Anna (CS, 2021) model from reducing to a non-singular matrix. The CS ATT is weighted over a seven-year event window to be comparable to my primary stacked difference-in-differences specification. The CS estimates are based on a never treated control group and probability weights estimated via OLS regression. Standard errors are clustered by county in all models and presented in parentheses. I drop all bonds with negative *Spread* and *Adjusted Spread* in Models 2-3. All variables are defined in Appendix B. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>		
	Yield (1)	Spread (2)	Adjusted Spread (3)
<i>Panel A: Inclusion of City Bonds</i>			
<i>Target</i> × <i>Post</i>	0.038 (0.026)	0.113** (0.048)	0.155** (0.063)
<i>Target</i>	-0.096** (0.040)	-0.087 (0.072)	-0.139** (0.067)
Controls	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes
Observations	598,187	376,327	545,791
<i>Adj R</i> ²	0.807	0.487	0.642
<i>Panel B: Exclusion of Additional Los Angeles Events</i>			
<i>Target</i> × <i>Post</i>	0.019 (0.036)	0.139** (0.070)	0.180* (0.100)
Controls	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes
Observations	348,393	204,807	319,973
<i>Adj R</i> ²	0.822	0.474	0.653

Table 9
(Cont.)

<i>Panel C: Inclusion of Bonds with Negative Spreads and Tax-Adjusted Spreads</i>			
<i>Target×Post</i>	0.050* (0.028)	0.172*** (0.070)	0.190*** (0.079)
Controls	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes
Observations	444,368	444,368	444,368
<i>Adj R²</i>	0.798	0.604	0.643
<i>Panel D: Neighboring Counties as Controls</i>			
<i>Target×Post</i>	0.028 (0.030)	0.128** (0.055)	0.160** (0.064)
Controls	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes
Observations	132,297	85,631	121,760
<i>Adj R²</i>	0.791	0.469	0.625
<i>Panel E: Propensity Score Matched Sample</i>			
<i>Target×Post</i>	0.157* (0.079)	0.233*** (0.103)	0.320** (0.119)
Controls	Yes	Yes	Yes
County×Event FEs	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes
Observations	5,102	5,102	5,102
<i>Adj R²</i>	0.845	0.666	0.705
<i>Panel F: Callaway and Sant'Anna (2021) Estimator</i>			
<i>Target×Post</i>	-0.008 (0.022)	0.198*** (0.027)	0.193*** (0.037)
Controls	Yes	Yes	Yes

Table 10. Descriptive Statistics for Municipal Bonds and Hospitals

This table presents summary statistics for my main sample of breached entities and their counterfactuals. Panel A presents statistics for my overall sample of bonds, and Panel B presents statistics related to hospital financial and balance sheet outcomes. Panel C describes 30-day patient readmission rates for my main patient outcomes, and Panel D overviews patients' self-reported care measures. Panel C presents statistics for my main sample of stacked county data. Each panel also names the source of the data. All continuous data are winsorized at the one percent levels.

Panel A: Overall Sample of Bonds (Mergent)

	N	Mean	SD	Pctl(25)	Median	Pctl(75)
Yield (%)	11,987	3.11	1.28	2.19	3.09	3.93
Adj Spread (%)	11,987	2.98	1.45	1.92	2.92	3.84
Issue Size (1,000s)	11,987	141,029.30	157,009.10	27,595.00	84,745.00	200,000.00
Bond Size (1,000s)	11,971	8,644.62	16,956.25	915	2,720.00	7,775.00
Coupon (%)	11,987	4.35	1	4	5	5
Maturity (Years)	11,987	11.91	7.36	6.34	10.42	15.78
Max Rating	11,987	9.1	4.58	5	8	14
GO	11,987	0.14	0.35	0	0	0
Callable	11,987	0.53	0.5	0	1	1
Negotiated	11,987	0.87	0.34	1	1	1
Tax Exempt	11,987	0.97	0.18	1	1	1
Population _{t-1} (1,000s)	11,987	1,008.22	819.03	435.49	799.68	1,485.22
Per Capita Income _{t-1} (1,000s)	11,987	44	9.61	37.94	41.89	48.87
Employment _{t-1} (1,000s)	11,987	647.42	511.82	252.14	752.77	841.53

Panel B: Hospital Financials (CMS Care Compare)

log Total Revenue (TR)	65,240	19.38	1.62	18.1	19.49	20.69
log Outpatient Revenue	65,280	18.33	2.15	17.23	18.82	19.85
log Inpatient Revenue	70,223	18.49	1.89	17.21	18.62	20.01
log Hospital Income	49,216	15.59	1.74	14.49	15.67	16.84
log Assets/TR _{t-1}	64,793	0.38	0.36	0.16	0.28	0.46
log Liabilities/TR _{t-1}	64,434	0.21	0.29	0.07	0.15	0.27
log Cash/TR _{t-1}	63,772	0.04	0.09	0.0001	0.01	0.05
log Fixed Equipment/TR _{t-1}	38,878	0.06	0.11	0.01	0.02	0.06
log Bed Days	74,181	10.54	1.1	9.69	10.64	11.39
Bed Utilization (%)	74,044	0.44	0.23	0.27	0.44	0.6

Panel C: Patient 30-Day Readmission Rates (CMS HCRIS)

Pneumonia	10,535	0.12	0.13	0.03	0.07	0.16
Heart Failure	9,572	0.2	0.2	0.05	0.11	0.28
Heart Attacks	5,670	0.16	0.15	0.05	0.1	0.21
COPD	9,670	0.19	0.18	0.06	0.11	0.26

Table 10
(Continued)

<i>Panel D: Patient Satisfaction of Care (CMS HCAHPS)</i>						
Recommend "Yes" (%)	8,173	70.08	10.1	64	70	77
Always Clean (%)	8,173	17.89	4.42	15	18	21
Doctor Always Clear (%)	8,173	80.06	6.02	76	80	84
Nurse Always Clear (%)	8,173	78.6	5.86	75	79	82
Recov Info Always Clear (%)	8,173	86.07	4.08	84	87	89
Room Always Quiet (%)	8,173	59.2	11.22	51	58	67
Rate "9-10" (%)	8,173	70.66	9.08	65	71	77

Table 11. The Determinants of Hospital Data Breaches

This table analyzes which characteristics are associated with hospital data breaches using a linear probability model. The dependent variable is a binary indicator that equals one if a hospitals' data are breached in a given year and zero otherwise, and all independent variables are both lagged and logged. Model 1 uses hospital and year fixed effects, and Model 2 replaces the fixed effects with county-year fixed effects to capture any effect the hospital's local economic environment has on its propensity to be breached. Standard errors are clustered by hospital in both models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable: 1(Breach)</i>	
	(1)	(2)
Total Revenue	0.001 (0.563)	-0.001 (-0.573)
Total Assets	0.001 (0.738)	0.001 (0.648)
Total Liabilities	0.0001 (0.388)	0.0003 (0.697)
Cash Holdings	0.0001 (0.653)	0.001** (2.536)
Full-Time Employees	-0.001 (-1.024)	0.002 (1.485)
Beds	-0.0004 (-0.445)	-0.0004 (-0.462)
Hospital FEs	Yes	No
Year FEs	Yes	No
County-Year FEs	No	Yes
Observations	26,670	26,670
<i>Adj R</i> ²	-0.007	-0.064

Table 12. Impact of Data Breaches on Cost of Hospital Financing

This table presents stacked triple difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, *Hack*, interactions between each pair of the variable, and an interaction between *Breach*, *Post*, and *Hack*. Models 2 and 4 include *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
<i>Breach</i> × <i>Post</i>	0.478** (1.98)	0.443** (2.48)	0.480 (1.38)	0.749*** (2.65)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	11,987	11,987	11,987	11,987
<i>Adj R</i> ²	0.472	0.893	0.476	0.789

Table 13. The Incremental Effect of External Hacks on Hospital Financing

This table presents stacked triple difference-in-difference coefficient estimates of my two main dependent variables on *Breach*, *Post*, and an interaction between *Breach* and *Post*. Models 2 and 4 include *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Model 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include issuer-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	-0.297 (-0.663)	-0.261 (-0.702)	-0.835 (-1.27)	-0.449 (-0.746)
<i>Breach</i> × <i>Post</i>	0.655** (2.29)	0.584* (1.87)	0.978* (1.89)	0.992** (1.99)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	11,987	11,987	11,987	11,987
<i>Adj R</i> ²	0.472	0.893	0.476	0.789

Table 14. Cash Flow Risk: Data Breaches and Hospital Health

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure hospital fundamental outcomes on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2015 and 2017 to ensure I have three years of pre- and post-breach outcomes. Each outcome is transformed by one plus the natural logarithm of the underlying variable. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	logarithm of 1 + <i>Dependent Variable</i>			
	Patient Revenue	Outpatient Revenue	Inpatient Revenue	Bed Utilization
	(1)	(2)	(3)	(4)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	-0.060*	-0.015	-0.101**	-0.023*
	(-1.684)	(-0.294)	(-2.342)	(-1.683)
<i>Breach</i> × <i>Post</i>	-0.009	-0.017	0.019	0.022*
	(-0.300)	(-0.409)	(0.614)	(1.962)
Total Effect	-0.068	-0.032	-0.082	0.002
<i>P</i> -Value	<0.001	0.152	0.001	0.842
Controls	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	44,665	44,663	44,665	44,645
<i>Adj R</i> ²	0.990	0.982	0.990	0.935

Table 15. Data Breaches and Patient Care Experience

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure how patients rate their experience while admitted to a hospital on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2017 and 2018 to ensure I have at least two years of pre- and post-breach outcomes and compare treated hospitals to control hospitals within the same county. Each outcome measures how patients perceive their experience at a hospital. Following Aghamolla et al. (2022), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by hospital in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable						
	Recommend "Yes"	Room Always Clean	Doc Comm Always Clear	Nurse Comm Always Clear	Recovery Info Always Clear	Room Always Quiet	Rate "9-10"
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	-1.369 (-0.546)	-1.015 (-0.866)	-1.065 (-0.699)	-0.124 (-0.074)	0.467 (0.351)	-1.650 (-0.846)	-1.972 (-1.287)
<i>Breach</i> × <i>Post</i>	0.612 (0.716)	0.979 (1.120)	0.746 (1.398)	-0.348 (-0.750)	0.761 (0.889)	0.844 (0.924)	0.602 (0.839)
Total Effect	-0.757	-0.036	-0.319	-0.472	1.228	-0.806	-1.369
<i>P</i> -Value	0.694	0.970	0.798	0.695	0.117	0.573	0.367
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5,861	5,861	5,861	5,861	5,861	5,861	5,861
<i>Adj R</i> ²	0.876	0.643	0.819	0.821	0.698	0.881	0.848

Table 16. Data Breaches and Patient Readmission Rates

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure patient readmission rates for various diagnoses on *Breach*, *Post*, *Hack*, and interactions between each of the terms. I include events between the years of 2017 and 2018 to ensure I have two years of pre- and post-breach outcomes and compare treated hospitals to control hospitals within the same county. Each outcome measures common measures of patient care quality, namely, the 30-day readmission rates for pneumonia (PN), heart failure (HF), heart attacks (AMI), and chronic obstructive pulmonary disease (COPD). The outcomes in Models 1-4 are transformed by the natural logarithm, and the outcomes in Models 5-8 are in percentage points. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. I compute the total effect of interaction terms and test for the sum's significance using a Wald chi-squared test. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by hospital in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	<i>Dependent Variable</i>							
	log(PN)	log(HF)	log(AMI)	log(COPD)	PN	HF	AMI	COPD
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
<i>Breach</i> × <i>Post</i> × <i>Hack</i>	0.148 (1.25)	-0.043 (-0.444)	0.347*** (3.50)	0.216** (2.27)	0.026* (1.77)	0.060* (1.75)	0.055*** (4.23)	0.050** (2.03)
<i>Breach</i> × <i>Post</i>	-0.144* (-1.83)	-0.116 (-1.61)	-0.302*** (-3.37)	-0.292*** (-4.18)	-0.009 (-0.983)	-0.023 (-0.974)	-0.040*** (-3.55)	-0.038* (-1.98)
Total Effect	0.003	-0.160	0.045	-0.076	0.018	0.036	0.015	0.012
<i>P</i> -Value	0.959	<0.001	0.002	0.156	0.057	0.089	<0.001	0.515
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	1,173	1,162	946	1,138	1,173	1,162	946	1,138
<i>Adj R</i> ²	0.995	0.995	0.996	0.993	0.968	0.966	0.989	0.972

Table 17. Yields and Hospital Financials around Periods of Interest in Data Breaches

This table presents stacked triple difference-in-difference coefficient estimates of several variables that measure the issuer cost of debt outcomes from Table 13 and hospital financial outcomes from Table 14 on *Breach*, *Post*, and *Hack* and interactions between each of the terms. The *Low Attention* (left) half of the table is based on a sample split of observations with less than the median search volume index (SVI), and the *High Attention* (right) half of the table is the complement. The variable *SVI* is the average yearly Google Trends search volume index for the phrase “data breach” in the hospitals’ respective states. I restrict base SVI on news articles to account for the spread of information regarding breaches and, therefore, the potential attention given to events. Following Aghamolla et al. (2023), I include the lagged variables *log Hospital Income*, *log Bed Days*, *Cash Holdings*, *log Liabilities*, and *Total Patient Revenue* as controls. The coefficients for the controls are omitted for brevity. I include hospital-event and year-event fixed effects in the models (Baker et al., 2022). Standard errors are clustered by issuer in all models, and *t*-statistics are presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Low Attention				High Attention			
Panel A: Hospital Financials								
	logarithm of 1 + Dependent Variable							
	Pat Rev (1)	Outpat Rev (2)	Inpat Rev (3)	Bed Util (4)	Pat Rev (5)	Outpat Rev (6)	Inpat Rev (7)	Bed Util (8)
Breach×Post×Hack	-0.062** (-2.30)	-0.011 (-0.310)	-0.095* (-1.85)	-0.018 (-1.21)	-0.127** (-2.10)	-0.068 (-0.593)	-0.135*** (-4.07)	-0.003 (-0.137)
Breach×Post	-0.006 (-0.235)	-0.011 (-0.387)	0.018 (0.430)	0.016 (1.51)	-0.013 (-0.233)	-0.046 (-0.459)	0.022 (0.800)	0.015 (0.878)
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	18,489	18,487	18,489	18,468	18,672	18,672	18,672	18,664
Adj R ²	0.992	0.986	0.990	0.951	0.990	0.983	0.991	0.938
Panel B: Issuer Cost of Debt								
	Yield		Adjusted Spread		Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Breach×Post	0.448 (0.669)	0.403 (1.56)	0.366 (0.477)	0.713* (1.77)	0.214 (1.47)	0.737*** (3.28)	0.474* (1.98)	1.23*** (3.34)
Controls	No	Yes	No	Yes	No	Yes	No	Yes
Hospital×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5,466	5,466	5,466	5,466	6,466	6,466	6,466	6,466
Adj R ²	0.534	0.933	0.597	0.853	0.355	0.847	0.316	0.727

Table 18. Robustness of Hospital Financing Tests

This table presents robustness tests for my main results in Table 12. I use a stacked difference-in-difference estimation in each model outside of those in Panel A, and the columns represent coefficient estimates of my three main dependent variables on *Breach*, *Post*, and an interaction between *Breach* and *Post*. Models 2 and 4 include *Coupon*, *Maturity*, *Inverse Maturity*, *Logged Issue Size*, *Callable*, *Negotiated*, *GO Bond*, *Tax Exempt*, *lag Population*, *lag Per Capita Income*, and *lag Employment* as control variables. Models 1 and 2 also includes the corresponding *Treasury Yield* as a control. The coefficients for the controls are omitted for brevity. I include state-event and year-event fixed effects in the models (Baker et al., 2022). Panel A presents my main financing test models using an alternative methodology (Borusyak et al., 2021) over the same sample period as my primary sample. Panel B presents the main results based on a coarsened exact matched sample. I split the continuous bond characteristics, county population, and county employment into four bins and match breached bonds to control bonds to those that are issued within the same year and bin and that have the same binary characteristics. Panel C presents the main results when using only non-breached issuers in the same county as the breached hospital as the control group. Standard errors are clustered by issuer in all models and presented in parentheses. All variables are defined in Appendix E. *, **, *** indicates significance at 10%, 5%, and 1% levels, respectively.

	Dependent Variable			
	Yield		Adjusted Spread	
	(1)	(2)	(3)	(4)
<i>Panel A: Alternative Estimator (Borusyak et al., 2023)</i>				
<i>Breach</i> × <i>Post</i>	0.364*** (5.02)	0.419*** (4.60)	0.821*** (6.93)	0.821*** (6.64)
Controls	No	Yes	No	Yes
Issuer FEs	Yes	Yes	Yes	Yes
Year FEs	Yes	Yes	Yes	Yes
Observations	16,416	16,416	16,416	16,416
<i>Panel B: Coarsened Exact Matched Sample</i>				
<i>Breach</i> × <i>Post</i>	0.805** (2.31)	0.536*** (4.29)	1.16** (2.13)	0.966*** (3.69)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	970	970	970	970
Adj R^2	0.323	0.913	0.377	0.814
<i>Panel C: Control Group of Non-Breached Issuers in Same County</i>				
<i>Breach</i> × <i>Post</i>	0.641** (2.32)	0.513* (1.90)	0.988* (1.82)	0.829** (2.08)
Controls	No	Yes	No	Yes
Issuer×Event FEs	Yes	Yes	Yes	Yes
Year×Event FEs	Yes	Yes	Yes	Yes
Observations	2,810	2,810	2,810	2,810
Adj R^2	0.424	0.843	0.360	0.723

Vita

Banks Osborne is a Ph.D. candidate in Finance at the University of Tennessee, Knoxville. He received his Bachelor of Arts in Economics, Bachelor of Science in Mathematics, and Masters of Science in Mathematics from the University of North Carolina Wilmington. Before joining the doctoral program, he worked as a statistical consultant for medical professionals and as a data scientist. His research interests include FinTech, cybersecurity, healthcare finance, municipal financing, and the real effects of financial markets.