

City Hall Has Been Hacked!

The Financial Costs of Lax Cybersecurity

Filippo Curti
Richmond Fed

Ivan T. Ivanov
Chicago Fed

Marco Macchiavelli
University of Massachusetts

Tom Zimmermann*
University of Cologne

July 17, 2024

*The views stated herein are those of the authors and are not necessarily the views of the Chicago Fed, the Richmond Fed, or the the Federal Reserve System.

Motivation

- ▶ State and local governments are attractive targets for cyber attacks:
 - ▶ Store and manage substantial amounts of personal identifiable information (PII)
 - ▶ Inadequate cybersecurity
- ▶ States and localities operate the nation's infrastructure
 - ▶ Cyberattacks such as data breaches more disruptive than attacks on corporates
- ▶ Data breaches have the potential to impose large welfare losses:
 - ▶ Remediation and litigation costs absorb public resources/taxpayer money
 - ▶ Negative externalities—leaked PII facilitates fraudulent activity

Cybersecurity at State and Local Governments

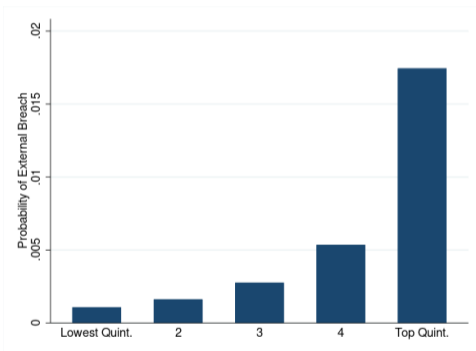
- ▶ Effect of data breaches on governments:
 - ▶ Negative abnormal bond returns in the secondary market
 - ▶ Increase in financing costs in the primary market
- ▶ The implementation of data breach notification laws at the state level:
 - ▶ Staggered implementation between 2002 and 2021 (penalties in some cases)
 - ▶ No effect on the incidence of future data breaches
 - ▶ Incentives to bolster cybersecurity may still be insufficient

Data

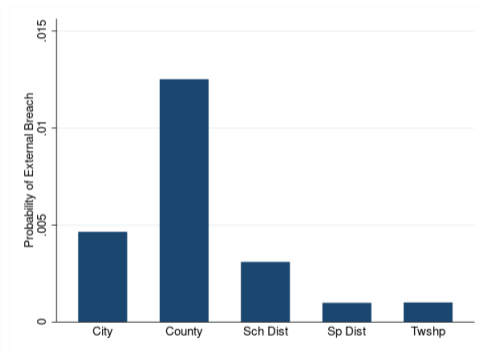
- ▶ Data on operational risk incidents (external and internal) from Advisen:
 - ▶ Over 1,000 attacked public entities, over 2,200 external data breaches since 2004
 - ▶ Bridge to other data via the Census of Governments
- ▶ Primary market issuance from Mergent:
 - ▶ Detailed information on bond characteristics, yields, and amounts.
- ▶ Secondary market data on municipal bond trading from the MSRB:
 - ▶ All transactions since 2010.
- ▶ Hand-collected data on state breach notification laws:
 - ▶ National conference of state legislatures (NCSL), LexisNexis
 - ▶ Enactment and effective dates, covered entities, penalties for violations (if any)

Data

- ▶ Risk of external data breaches across government size and type.



A. Government Size



B. Government Type

Data Breaches and Abnormal Bond Returns

- ▶ We follow (Cornaggia, Hund, and Nguyen 2022) to estimate abnormal returns:

$$r_{b,s,k} = (D_{b,s} \cdot y_{b,s} - D_{b,k} \cdot y_{b,k})$$
$$ar_{b,s,k} = r_{b,s,k} - \sum_{t=k+1}^s R_t^l$$

- ▶ $y_{b,t}$ ($D_{b,t}$) yield to maturity (duration) of bond b at time t
- ▶ $r_{b,s,k}$ duration-adjusted return on bond b btw two adjacent trades, s and k
- ▶ Index return, R_t^l , l denotes remaining maturity–credit rating buckets

Data Breaches and Abnormal Bond Returns

- ▶ Negative abnormal returns around external data breaches of about 16-17 bps.

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

Data Breaches and Abnormal Bond Returns

- ▶ Returns larger in magnitude for subordinated bonds.

Abnormal bond returns and bond heterogeneity

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

Data Breaches and Abnormal Bond Returns

- ▶ Returns slightly larger for entities with higher 'attack surface'.

Panel B: Abnormal Bond Returns and Government Type

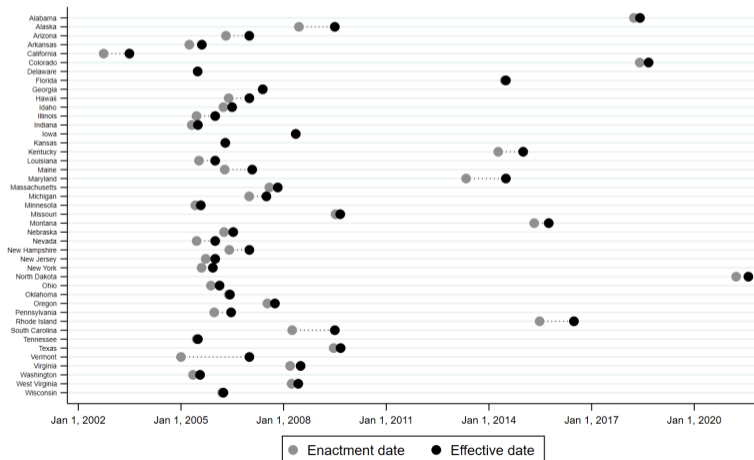
Govt Type	City/Twp	County	District	State
Bond Return	-16.976*** (1.509)	-21.722*** (3.241)	-15.215*** (5.613)	-19.235*** (4.997)
Observations	26,036	5,210	1,439	2,940
Number of Events	1,372	609	213	378

Data Breaches and Issuance Costs

- ▶ Primary markets provide unique insights into consequences for taxpayers
- ▶ Use yields of muni bond offerings as a measure of issuance costs
- ▶ Offering yields increase by about 10 bps after cyberattacks
- ▶ Effects are persistent

Data Breach Notification Laws

- ▶ Most states now have data breach notification laws
- ▶ Public entities required to notify residents of data breaches



Data Breach Notification Laws

- ▶ Role for regulation?
 - ▶ Higher financing costs detract resources from the community
 - ▶ Loss of personal data increases chance of fraud
 - ▶ Regulation may incentivize investment in cybersecurity by penalizing breaches

Data Breach Notification Laws

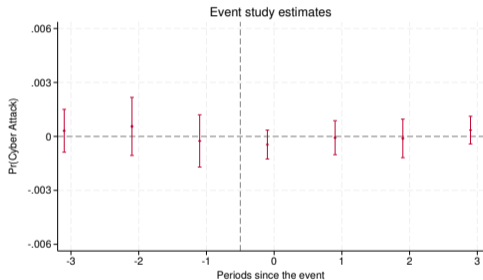
- ▶ Use the Borusyak, Jaravel, and Spiess (2021) estimator:

$$Y_{i,s,t} = \sum_{j=-3}^3 \beta_j Law_{s,t+j} + \mu + \epsilon_{i,s,t}$$

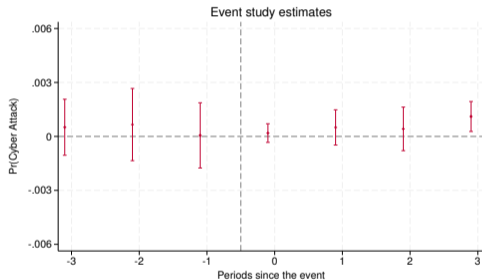
- ▶ $Law_{s,t+j}$ equals one if entity i in state s is covered by law is enacted j years ago
- ▶ treatment whenever law allows for monetary penalties and apply to local govt

Effect of Data Breach Notification Laws

C. Prob. of Cyberattack (Local)



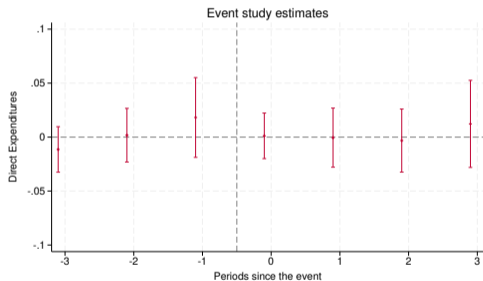
D. Prob. of Cyberattack (Any)



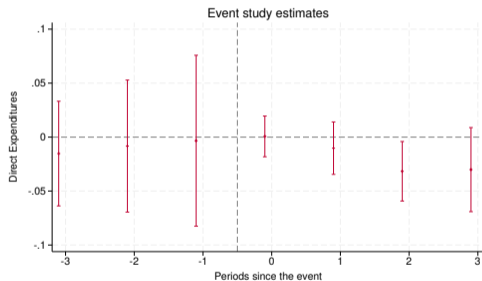
- ▶ No improvement in cybersecurity
- ▶ No significant reduction in the likelihood of future data breaches

Effect of Data Breach Notification Laws

A. Direct Expenditures (Local)



B. Direct Expenditures (Any)



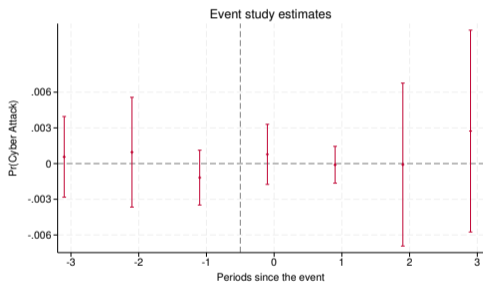
- ▶ No spending changes around the implementation of breach notification laws

Data Security Laws

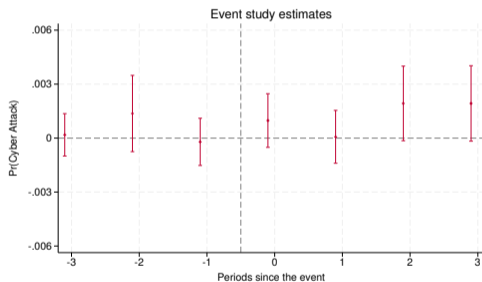
- ▶ Explicit requirements for governments to strengthen cybersecurity
- ▶ A state oversight body that:
 - ▶ sets cybersecurity standards
 - ▶ conducts audits and employee training
- ▶ Greater potential incentive effects to strengthen cybersecurity

Effect of Data Security Laws

A. Prob of Cyberattack (Local)



B. Prob of Cyberattack (Any)



- ▶ No significant reduction in the likelihood of future data breaches

Effectiveness of State Cybersecurity Laws

- ▶ Data breach notification laws not associated with better cybersecurity
- ▶ Tradeoff between ex-ante cost to improve cybersecurity + ex-post remediation costs
- ▶ Alternative incentive schemes:
 - ▶ Safe harbor against data breach lawsuits if comply with industry-recognized cybersecurity programs
 - ▶ Possibly providing incentives to invest ex-ante

Conclusion

- ▶ Significant costs of neglecting cybersecurity
 - ▶ Data breaches expose municipalities to additional financing costs
 - ▶ This is in addition to the loss of privacy and fraud
- ▶ Data breach laws appear ineffective at reducing cyber risk:
 - ▶ Do not reduce the likelihood of future external data breaches

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

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