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

April 12, 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

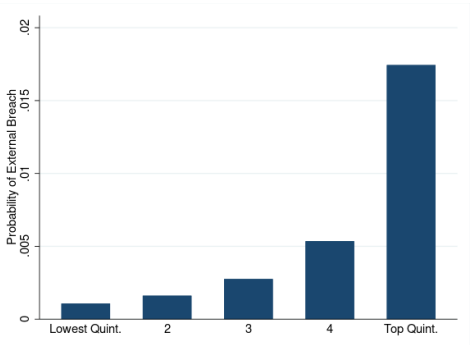
- Effect of data breaches on governments:
  - Negative abnormal bond returns in the secondary market
  - Increase in financing costs in the primary market
- The implementation of data breach notification laws at the state level:
  - Staggered implementation between 2002 and 2021 (penalties in some cases)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

Data

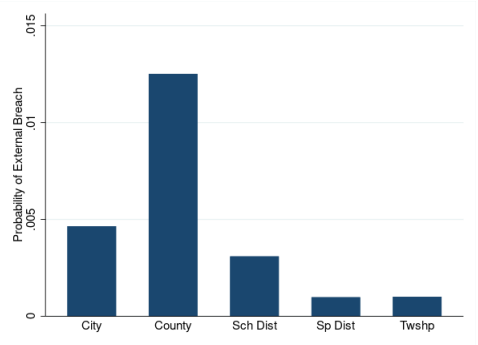
- Data on operational risk incidents (external and internal) from Advisen:
  - Over 1,000 attacked public entities, over 2,200 external data breaches since 2004
  - Bridge to other data via the Census of Governments
- Primary market issuance from Mergent:
  - Detailed information on bond characteristics, 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

- Examine the bond response to data breaches using an event study approach:

$$r_{b,s,k} = (D_{b,s} \cdot y_{b,s} - D_{b,k} \cdot y_{b,k})$$

$$ar_{b,s,k} = r_{b,s,k} - \sum_{t=k+1}^{s} R_t^l$$

  - $y_{b,t}$ ($D_{b,t}$) 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***	-17.744***	-5.301***
	(2.433)	(1.295)	(1.516)
Observations	36,179	35,679	35,677
Number of Events	2,582	2,573	2,573

Data Breaches and Abnormal Bond Returns

- Returns similar across different types of bonds.

Abnormal bond returns and bond heterogeneity

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

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

$$Y_{i,t} = \sum_{j=-2}^{j\geq+3} \beta_j Breach_{i,t+j} + \delta X + \mu + \epsilon_{i,t}$$

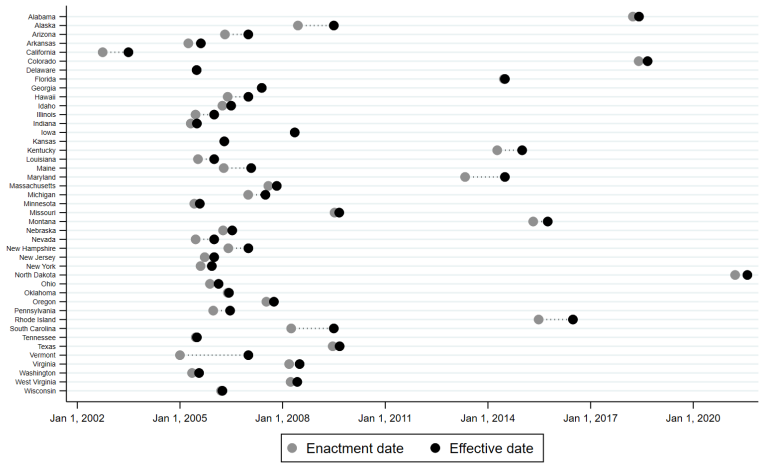
  - $Y_{i,t} = \{$bond issuance, yields, offering type$\}$
  - $Breach_{i,t+j} = 1$ if government i suffers an external data breach in year $t + j$
  - government type-year, state-year, entity FEs & size controls

External Data Breaches and Primary Bond Markets

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

Data Breach Notification Laws

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



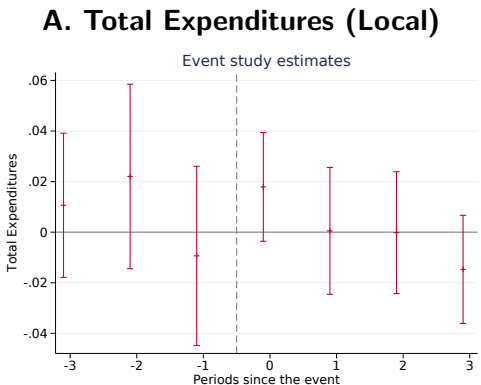
Data Breach Notification Laws

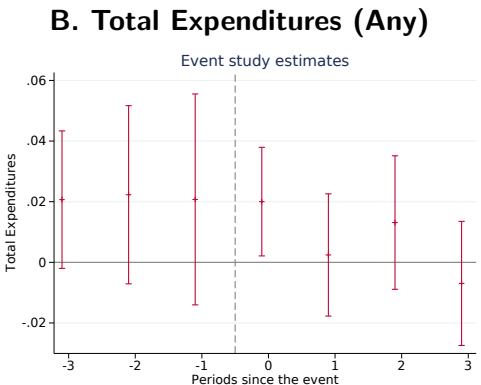
- Role for regulation?
  - Higher financing costs detract resources from the community
  - Loss of personal data increases chance of fraud
  - Regulation may incentivize investment in cybersecurity by penalizing breaches

$$Y_{i,s,t} = \sum_{j=-2}^{4+} \beta_j Law_{s,t+j} + \mu + \epsilon_{i,s,t}$$

  - $Law_{s,t+j}$ 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

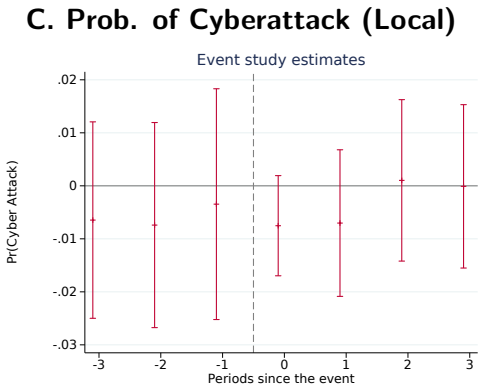
Effect of Data Breach Notification Laws

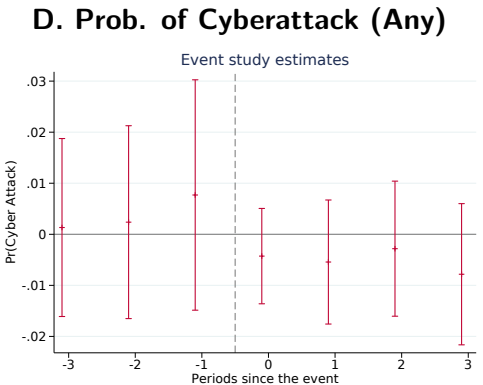




- Temporary increase in expenditures in the enactment year

Effect of Data Breach Notification Laws





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

Effectiveness of Breach Notification

- 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 and expenditures
  - This is in addition to the loss of privacy and fraud
- Data breach laws appear ineffective at reducing cyber risk:
  - They do not reduce the likelihood of future external data breaches