ChicagoFedLetter

September 2024, Number 501
https://doi.org/10.21033/cfl-2024-501

Exposure to cyber risk and inadequate cybersecurity regulations: Evidence from municipalities

Filippo Curti, financial economist, Federal Reserve Bank of Richmond, Ivan Ivanov, senior economist, Marco Macchiavelli, assistant professor of finance, Isenberg School of Management, and Tom Zimmermann, professor of data analytics, University of Cologne

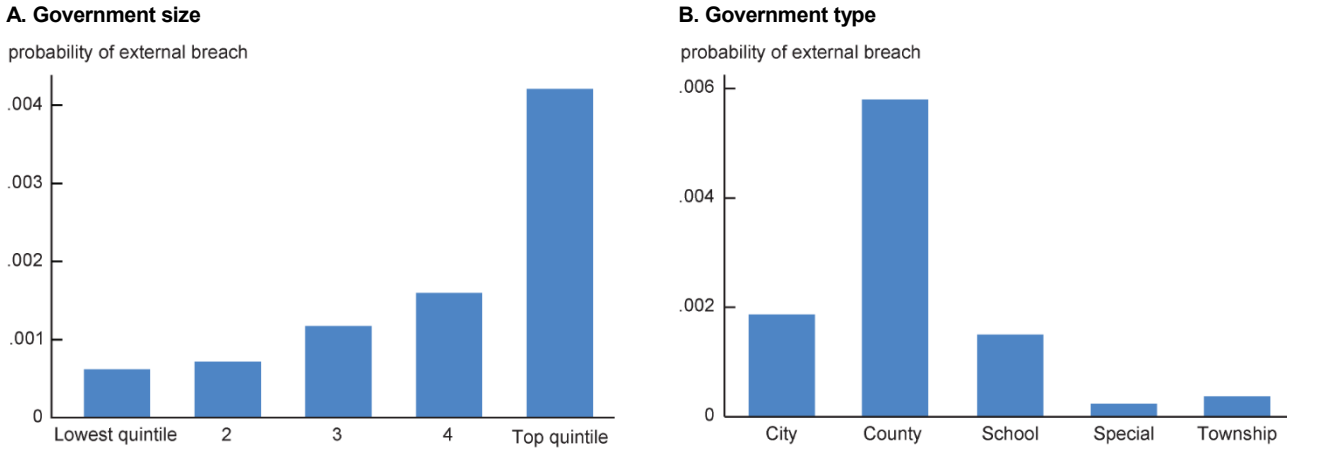
In this article, which is based on a related working paper, we document the adverse effects of cyberattacks on municipalities and the ineffectiveness of current state regulation to stave off future cyberattacks. In the process of providing services to their citizens, state and local governments collect and store a wide range of sensitive personal information (data). Access to personal information, sometimes combined with a lack of adequate cybersecurity (FitchRatings, 2022), makes governments attractive targets for cyberattacks, in particular data breaches. Indeed, in our sample external data breaches represent the most common source of cyber risk for governments; therefore, we focus primarily on them.

We find that following a cyberattack, municipalities experience an increase in financing costs on new bond issuance, as well as a reduction in the price of outstanding bonds. A conservative estimate indicates that cyberattacks cost municipalities nearly $60 million in additional interest costs per year. Relatedly, municipal bond investors have suffered over $1.5 billion in mark-to-market losses due to cyberattacks on average each year. In addition to these financial costs, cyberattacks impose additional costs on municipalities, including litigation and remediation costs. They also expose sensitive personal information to hackers, who monetize the stolen data in various ways, including credit card fraud and tax refund fraud.

In response to the increasing threats posed by cyberattacks, since the early 2000s most U.S. states have enacted some form of cybersecurity regulation that applies to state and local governments. These laws belong to two major groups: data breach notification and data security laws.[1] We show that both data breach notification laws and data security laws have little impact on the probability of future cyberattacks on governments. Finally, we discuss some recent alternative regulations that may better align incentives to invest in cyber defenses.

Altogether, cyberattacks appear to impose substantial remediation and litigation costs on governments, which adversely affect their municipal bond valuations and external financing costs. Lax cybersecurity is therefore a significant source of risk for bond holders, and the associated costs may divert funding from public infrastructure and services.

1. External breaches across government size and type



Sources: Advisen—A Zywave Company and U.S. Census Bureau, Annual Survey of State and Local Government Finances.

Data breaches affecting state and local governments: Some facts

Among the approximately 90,000 state and local governments with available balance-sheet information, 1,011 distinct entities faced a total of 1,551 external data breaches between 2004 and 2019. Out of the 1,011 governments with external data breaches, 853 were attacked once, 83 twice, 17 three times, and the remaining 58 were attacked four or more times during the sample period. States are the most likely targets (all but two states are attacked at least once), followed by counties and school districts, roughly 5% and 3% of which, respectively, were attacked at least once. Finally, cities, special districts, and townships have a significantly lower probability of ever being attacked, hovering at around 1% or less.

As shown in figure 1 (panel A), the probability of an external data breach increases with government size. On average, only less than 0.1% of governments in the bottom quintile of the total revenue distribution face a data breach in any given year. In contrast, over 0.4% of the largest governments have at least one external data breach in any given year. Panel B of figure 1 breaks down cyber incidents by government type, such as cities, counties, school districts, special districts, and townships. City, county, and school district governments experience external data breaches a lot more frequently than township and special district governments.[2] While these results are likely attributable to the size differential from panel A, general-purpose governments, such as cities and counties, maintain a wider array of sensitive personal information, which may expose them to greater cybersecurity risk than special-purpose entities.

Data breaches and bond yields

Data breaches have a detrimental effect on municipal bonds. We find that bond prices in the secondary market based on transactions data from the Municipal Securities Rulemaking Board (MSRB) decline significantly within 30 days of a data breach. We estimate a value-weighted negative abnormal return of 8.3 basis points following a cyberattack. A back-of-the-envelope calculation suggests that municipal bond investors suffered a total of nearly $15.6 billion in mark-to-market losses due to external data breaches between late 2010 and early 2020. Mark-to-market losses to municipal bond investors associated with ransomware and distributed denial of service (DDoS) attacks amounted to nearly $1.5 billion over the same period. We also examine the effect of data breaches on bond prices in the primary market. This analysis is most applicable to large and frequent bond issuers, such as states and major cities, given the typical issuer raises bond financing only infrequently. We find that primary market yields are persistently higher by about 6–7 basis points after a data breach, which represents about a 2.4% increase relative to

the average bond yield in our sample. A conservative back-of-the-envelope estimate suggests an additional $809 million in interest costs on municipal bond offerings between 2004 and 2017. We arrive at this estimate by multiplying 7.1 basis points, the $1.897 trillion in total municipal bond issuance between 2004 and 2017, the average duration of 6.13 years of sample bonds assuming they will be called at the earliest call date, and the value-weighted average cyberattack probability of 9.8% in the year of issuance. This deadweight loss was eventually borne by taxpayers and could have been mitigated with stronger ex ante cyber defenses. Our estimates are similar to those associated with other emerging risks in the municipal bond market, such as flood risk, rising health care costs, or anti-ESG (environmental, social, and governance) legislation that the literature estimates at 5 to 12 basis points of municipal bond yields (Goldsmith-Pinkham et al., 2023; Gao, Lee, and Murphy, 2022; and Garrett and Ivanov, 2024).

The likely channel: Remediation and litigation costs

The detrimental effect on bond prices is consistent with data breaches increasing governments' operating expenses, such as remediation costs to restore computer networks and litigation costs associated with fines and damages resulting from the data breach. For example, a global survey of corporations shows that data breaches translate to increases in insurance premiums, external hiring, staff training, legal costs and fines, and improvements in IT systems, as discussed in Kaspersky (2018). We corroborate this idea by showing that total and direct expenditures of governments increase significantly—by between 1.5% and 1.8%—in the year of a cyberattack.

Externalities and a role for cyber regulations

In addition to litigation, remediation, and financial costs, cyberattacks expose people to a loss of privacy, with the stolen identifiable information often monetized via credit card fraud or tax refund fraud. Given the substantial negative externalities of cyberattacks, there is room for regulations to incentivize municipalities to shore up cyber defenses.

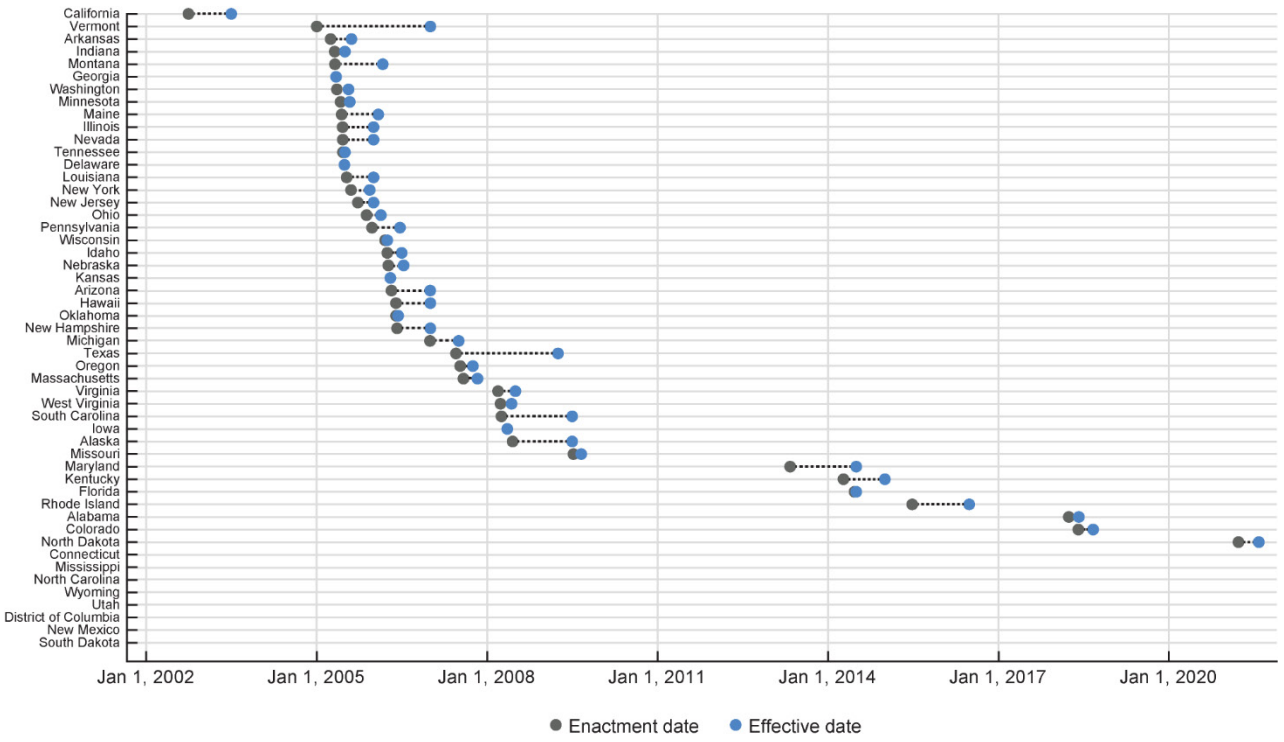
Data breach notification and data security laws

Most U.S. states have introduced data breach notification laws since the early 2000s (see figure 2). These laws require governments affected by a data breach to notify the public of external data breaches in a timely manner. Data breach notification laws vary significantly across states, with some laws applying only to state agencies while others apply to both state and local government entities. A moderate increase in litigation risk and monetary penalties arising from data breach notification laws may incentivize municipalities to invest in cybersecurity, thereby reducing the number of cyberattacks. At a minimum, notifying citizens of a data breach requires at least a basic level of cybersecurity so that governments detect breaches. Separately, states have also passed data security laws, which introduce more-explicit guidelines to state and local government entities on how to secure their information systems against data breaches. These laws typically establish a state oversight body tasked with setting security standards and conducting security audits and employee training.

Effect of cyber regulations

We find that both data breach notification laws and data security laws did not attenuate the incidence of future external data breaches for municipalities. That said, our empirical tests do not allow us to rule out the possibility that notification and data security laws, while not affecting the future incidence of cyberattacks, may still mitigate their severity, namely the amount and sensitivity of the data obtained in the breach.

2. Staggered implementation of data breach notification laws by state



Sources: National Conference of State Legislatures and LexisNexis.

Policy implications

Investment in cybersecurity infrastructure reduces ex-post remediation, litigation, and financing costs to the extent that such investment lowers the ex ante probability or severity of future cyberattacks. Consequently, regulation requiring cybersecurity infrastructure investment may be beneficial if it requires industry-recognized cybersecurity programs that are considered best practice. Such programs may decrease the incidence and severity of data breaches, thus mitigating ex post litigation and financing costs, as well as the loss of privacy that accompanies data breaches. However, municipalities may not have enough incentives to front-load these cybersecurity investment costs, especially if they do not perfectly shield them from attacks. Indeed, the worst-case scenario for municipalities would be to pay the ex ante investment costs as well as the ex post litigation, remediation, and financing costs. Therefore, providing incentives to municipalities to invest in cybersecurity ex ante, instead of only in the aftermath of a successful attack, may reduce cybersecurity risk in a meaningful way. Recent laws that incorporate incentives to make ex ante cybersecurity investments have been passed in a few states (McGladrey, 2021). These laws give companies and municipalities a safe harbor against data breach lawsuits if they comply with industry-recognized cybersecurity programs.

Notes

[1] While data breach notification laws may be primarily intended to make citizens aware of cyberattacks, they may nevertheless increase governments' incentives to strengthen cyber defenses.

[2] Special districts are independent units that perform a specific service for a defined area, such as fire protection or water provision.

Chicago Fed Letter is published by the Economic Research Department of the Federal Reserve Bank of Chicago. The views expressed are the authors' and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.

Daniel G. Sullivan, Economics Editor; Helen Koshy and Han Y. Choi, Editors; Julia Baker, Senior Production Editor; Sheila A. Mangler, Editorial Assistant.

ISSN 0895-0164