Bond Case Briefs

Municipal Finance Law Since 1971

What Cyberattacks Do To Municipal Issuers' Borrowing Costs: Brookings

State and local governments are frequent targets of cyberattacks. In "City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity," a paper presented at the 2024 Municipal Finance Conference at Brookings, four economists find that municipal borrowing costs rise after a publicly reported cyberattack.

Filippo Curti (Federal Reserve Bank of Richmond), Ivan Ivanov (Federal Reserve Bank of Chicago), Marco Macchiavelli (University of Massachusetts, Amherst), and Tom Zimmermann (University of Cologne) use data breach and ransomware data on over 1,000 cyberattacks against public entities between 2004 and 2018 from Advisen, a data provider for insurers. They matched government victims of cyberattacks with data from the Census of Governments and from the Mergent Municipal Securities Database and the Municipal Rulemaking Standards Board.

After a data breach, they find, the bond prices of the target issuer in the secondary market decline between 15 to 22 basis points and primary market yields rise by 10 to 13 basis points, which is 5% higher than average bond yields in their sample. Governments hit by data breaches are much more likely to negotiate prices of new bond offerings, but they find no evidence that data breaches affect the size of bond offerings.

Curti and co-authors show that cyberattacks lead to roughly $1.77 billion in mark-to-market losses to municipal bond investors on the $870 billion in outstanding bonds of issuers hit by data breaches between 2010 and 2019. This estimate, they say, is likely a lower bound, because many bonds of issuers affected by cyberattacks may be illiquid and not trade in the 60-day window studied.

The authors also examine the effect of state data breach notification laws, which require targets of cyberattacks to notify residents, and data security laws, which mandate measures to strengthen cybersecurity. The authors find that both types of laws temporarily increase government expenditures to comply with new rules, but do not change the likelihood of future data breaches.

Since the laws are proven to not be enough to prevent future cyberattacks, Ivanov proposed at the conference that alternatives should be considered. One option is to give "a safe harbor against data breach lawsuits if the government entity complies with industry-recognized cybersecurity programs." Such an approach would incentivize upfront investment in cybersecurity, safeguarding personal and important information of the public, and potentially reduce the long-term financial losses from cyberattacks.

The Brookings Institution

by Tristan Loa and David Wessel

August 7, 2024