Bond Case Briefs

Municipal Finance Law Since 1971

Cyberattacks On Municipalities Can Tank Your Bond Portfolio.

When you think of cyberattacks you probably assume attacks on your bank account, your credit cards, or your brokerage accounts. There's a new risk. Now, when you hear of such breaches add your municipal bond issuers to the victim list.

Ransomware—the weapon of choice

Cyberattacks use ransomware viruses as the preferred infection vector. This is now an enormous risk to municipalities that issue bonds. These include cities, water districts, wastewater facilities, hospitals, utilities—really any entities that issue municipal bonds.

Don't for one minute think that such attacks are only inflicted on small cities or systems. The city of Atlanta was hacked and it affected nearly 6,000,000 people.

Hackers recently stole the infamous Stuxnet cyber worm developed and deployed to attack Iran's nuclear centrifuges. Somehow this cyber-weapon got out into the wild and is now among the hacker's tool of choice. Hackers have breached the city of Baltimore's computers. Erie County Medical Center in New York was hacked, bringing down the computer that ran their level one trauma center for six weeks.

The thread of commonality is simple: cyber criminals hack a facility, disable it, demand a ransom often in untraceable bitcoin, then promise to release the data after payment. That may or may not happen.

Municipalities as cyber-attack targets

Cyber criminals hack large and small systems, creating total chaos. It's easy to understand the necessity for computer assistance at hospitals. Cities, on the other hand, are more difficult. In the Baltimore hack residents couldn't pay water bills or parking tickets. Permits of all kinds were held up. There were no government emails nor emergency services deployed via the automated dispatch system. In other words, things ground to a halt. Baltimore's cost of recovery was around $18 million—money for which the city hadn't budgeted.

The small city of Riviera Beach, Florida (population 35,000) was hacked with a ransom demand of $600,000 payable in bitcoin. Riviera Beach had cyber ransom insurance. Still, like any policy questions arose of how quickly the insurance company would pay the ransom. In general, insurance payoffs take weeks. There may also be protracted litigation. Not a good thing when critical systems are down.

Now mix into all these cyberattacks the very real risk that even if the hospital, utility, city, or water district pays the ransom, will the frozen data be released. Maybe, maybe not. Cybercriminals have proven themselves totally untrustworthy.

Risk to investor’s bond portfolios

At Envision Capital we once had a client who transferred into his account municipal bonds issued by a city that was hacked. The city paid the outsized ransom. Still, questions arose as to what this will do to that city’s finances and to its credit rating.

It’s imperative that you connect the dots regarding your individual municipal bonds. If a city council, hospital board, or utility commission does not have updated cybersecurity then your investment is on borrowed time. Disabling any of the aforementioned entities means lost revenue, ransom they probably cannot pay, insurance that may or may not pay, uncollected bills, missed payroll—the falling dominos can be numerous.

Protecting your bond portfolio

The only way to protect yourself as a municipal bond investor is to keep your allocations between 3%-5% in any single large or medium-sized hospital, utility, city, water district, or other municipal issuer. Over-allocating beyond that maximum range allows a cyber hack that kidnaps the issuer’s computer systems and holds them for ransom to have a worse effect on your bond portfolio than it should.

As hackers test vulnerabilities of cities, municipal systems, infrastructures, and facilities the underlying municipal bonds are in jeopardy. It’s a bond investor best practice to add cyberattacks to your list of municipal credit risks.

Forbes

by Marilyn Cohen

Jun 25, 2019