Bond Case Briefs

Municipal Finance Law Since 1971

How Cybersecurity is Factoring Into Credit Ratings.

Cyberattacks are an emerging factor in public finance credit ratings for state and local governments, governmental authorities and non-profit community groups.

A couple of states already have stepped forward to help smaller communities and governmental authorities cope and about two dozen have formed state task forces.

A growing number of communities and government agencies also have taken out cybersecurity insurance policies.

“State and local governments are soft targets because they don’t have the expertise in cybersecurity that corporations do,” said Michael Belsky, executive director of the Center for Municipal Finance at the University of Chicago.

“I would say that being adequately prepared for a cyber event is a positive credit factor and being ill prepared is a negative credit factor,” Belsky said in an interview.

Credit rating agencies are looking at the quality of the computer systems personnel and whether a government entity has a plan to deal with cybersecurity.

“It’s more like a management practice like fund balance policy or revenue forecasting,” Belsky said.

The first hard evidence of how this is affecting ratings in the public finance sector came from a downgrade two months ago involving Princeton Community Hospital in West Virginia.

S&P Global Ratings lowered its rating to BBB from BBB+ on series 2012A refunding bonds in November, more than two years after a cyberattack weakened the hospital’s reserves which already were declining because of operating losses. Another factor in the downgrade was the integration risk associated from the acquisition of a regional medical center.

When the attack occurred in June 2017, the hospital had to divert ambulances and limit its services for seven weeks because the ransomware attack froze all systems including billing, accounting and electronic medical records.

Although S&P said the hospital’s management “responded appropriately” to the cyberattack and the hospital did not violate its debt service covenants in fiscal 2018, the incident provides a good example of how a cyberattack can factor into bond ratings.

“We are saying now that an attack has affected operations of a public finance entity to be the primarily the attribute to lead directly to the downgrade,” said Geoff Buswick, S&P Global Ratings managing director.

“We have watched this emerge over the past few years,” said Buswick. “Now it’s something that we are expecting every analyst to at least ask a question or two about on a call so it’s more business as usual.”

Moody's Investors Service hasn't downgraded any of its ratings because of cybersecurity risks as yet, but officials there said it could happen in the future.

"A lot of the losses have minimized because of cyber insurance or state support," said analyst Nisha Rajan, Moody's lead for ransomware attacks on local governments. "Smaller local governments tend to be more vulnerable because their budgets are smaller and there are less resources to tap."

A Moody's report last August highlighted the state support Louisiana provided when five school districts came under cyberattack.

Louisiana Gov. John Bel Edwards declared a state of emergency and the targeted school districts gained access to state resources from the Louisiana National Guard, Louisiana State Police, Louisiana Office of Technology Services and Louisiana State University.

The effort was coordinated by the governor's office of Homeland Security & Emergency Preparedness.

Similarly, the Moody's report noted that Colorado Gov. John Hickenlooper declared a state emergency in March 2018 following a ransomware infestation at the Colorado Department of Transportation.

Louisiana's response was aided by the fact that Gov. Edwards had established the Louisiana Cybersecurity Commission in 2017. About two dozen states have taken a similar step, including California, Texas, New York and Illinois.

Ohio received a credit positive from Moody's in November after Gov. Mike DeWine signed legislation creating a civilian cybersecurity reserve force, named the Ohio Cyber Reserve, to protect local governments, critical infrastructure and businesses from the impact of cyberattacks.

The 50 person unit is part of the Ohio National Guard.

Moody's said it "underscores the significant role states can play in helping governments respond to rising cybercrime."

The vulnerability is generally the greatest in smaller local governments and agencies.

"You have some state and local governments that are well-resourced that are able to mount a comparable defense to large private organizations," said Leroy Terrelonge, assistant vice president and cyber risk analyst at Moody's Investors Service.

"But you have in this large world of state and local governments you many that do not have the resources to have dedicated cyber expertise and to be able to protect themselves as well," Terrelonge said. "So when you have such a large attack surface for criminals that are looking to find weak links they can probe, it's a very rich target landscape."

At Fitch Ratings, cybersecurity risk is a factor in its ratings but not to the point where it has become a credit concern as yet, according to Managing Director Amy Laskey.

"We look at their general ability to deal with the unexpected as part of their ESG score," said Laskey.

Laskey the risk of cyberattacks is growing everywhere.

“There’s going to have to be a lot more done to address it, as these events become more common and more sophisticated and potentially more impactful,” Laskey said. “It’s probably going to get worse and not better so the responses are going to have to get stronger.”

The latest warning of the growing threat of cyberattacks came from the U..S. Department of Homeland Security and the Multi-State Information Sharing and Analysis Center shortfall after the U.S. killed Iranian Gen. Qassem Soleimani with a drone attack.

“The Iranians probably don’t have military capabilities to fight person for person or weapon system for weapons system, but they have a very sophisticated cybersecurity wing,” Buswick said.

On Jan. 7, Texas Gov. Greg Abbott and Texas Department of Information Resources executive director Amanda Crawford reported as many as 10,000 “probes” per minute of state agencies’ computer systems that originated from Iran.

“That whole chain of events was pretty stunning and telling to what we have been warning,” said Buswick. “Don’t have your head in the sand on this. Prudent cyber hygiene is going to benefit everyone.”

By Brian Tumulty

BY SOURCEMEDIA | MUNICIPAL | 01/14/20 02:35 PM EST