Bond Case Briefs

Municipal Finance Law Since 1971

Can a Cyberattack Cause a Credit Rating Downgrade?

While it seems far-fetched, the danger is real for small governments.

Last month saw an unprecedented global ransomware attack that infected tens of thousands of computers in nearly 100 countries, including the U.S., the U.K. and Russia. Hospitals in the U.K. were the hardest hit as more than a dozen were forced to turn away nonemergency patients and doctors had to rely once again on pen and paper.

The disruption has caused many to consider how vulnerable U.S. government services are to a similar attack. But some are raising the possibility of another vulnerability: That a cyberattack has the potential to lower a government's credit rating, making borrowing to fix the problem even more expensive for taxpayers.

The possibility seems remote: No government yet has been downgraded because of a cyberattack. But S&P Global Ratings analyst Geoff Buswick says the risk is real, particularly for smaller governments with less financial flexibility. That's because attacks can cost a lot, but can also cost taxpayer trust. That in turn, can hinder a government's ability to raise taxes. "As a rating analyst, I look at the willingness and ability to repay debt," says Buswick. "Without taxpayer support you don't have that ability."

The concerns come as ransomware attacks — malicious software that blocks computer system access until a ransom is paid — have been on the rise. According to the U.S. Department of Justice, an average of more than 4,000 ransomware attacks per day occurred in 2016, a 300 percent increase over the prior year.

This year alone, the St. Louis Public Library; Licking County, Ohio; the library server system for Hardin County Schools, Tenn.; Bingham County, Idaho; and the network of the Pennsylvania Senate Democratic Caucus were all victims of a ransomware attack.

The success of such attacks vary. In St. Louis, the library had backups for the encrypted files and refused to pay the ransom.

But more sophisticated attacks on smaller governments can bring more damage. In Bingham County, which is not rated, a ransomware attack in mid-February brought down the county's website and disrupted the emergency dispatch center. The problems persisted for weeks as officials worked to rebuild the county's computer infrastructure to avoid paying the $28,000 ransom. In the end, though, it agreed to pay a $3,500 ransom to the hackers in early March after officials determined that it would be cheaper than buying new servers.

But the ransom was just the tip of the financial damage. Bingham County's IT Department told the East Idaho News that the cost of repairing the servers was nearing the $100,000 mark, and that it could take the remainder of the year to get back to normal. For a county with less than $1 million in reserves, the unplanned expense cuts into the government's financial flexibility, a key credit rating measure.

Often, the monetary damage can be bigger. In spring 2016, the city-owned Lansing, Mich., Board of Water & Light paid a $25,000 ransom to unlock its internal communications systems. The utility, which is rated, reported six months later that responding to the attack cost the city $2.4 million, all but $500,000 of which was covered by insurance.

Buswick notes that the Lansing utility was large enough to absorb the damage but says others might not be in that position. Utilities have monthly income but school districts, for example, only get their revenue twice a year. “[The utility] had to use some of the reserves they were not on using,” he says. “In another situation, credit could be an issue.”

GOVERNING.COM

BY LIZ FARMER | JUNE 7, 2017