Bond Case Briefs

Municipal Finance Law Since 1971

Cybersecurity: Is It Enough of a Factor in Credit Risk Analysis?

This report has been prepared by Court Street Group Research.

In light of the recent attacks on Atlanta and Baltimore's municipal computer systems, investors in municipal debt should start to consider the protective measures being undertaken by municipalities to deter future attacks.

Which elicits the question: Should the issue of cybersecurity be more explicitly addressed by raters and investors as a component of the analysis of creditworthiness and relative value?

We have noted more than once the lack of significant reference to the issue in offering documents and financial statements. Though, ratings agencies do sometimes reference the issue in general statements. What we do not see is a truly granular analysis of how cybersecurity vulnerabilities could affect a municipality's underlying credit. Perhaps this is because there has not been a significant enough cost — operationally or financially — to stimulate the effort. It could also be seen as reflective of a view expressed in some rating agency comments that puts these events on a par with natural disasters. This would seem to imply reliance on a federal response to the financial implications of a large-scale financial attack.

We see a major weakness in that approach. The first is that the frequency and cost associated with natural disasters seems to be on an ever-rising upward curve. This has made each response to these events more contentious politically as the approval process for appropriations of federal dollars to support recovery efforts become more intertwined with general budget politics. More important is the recent public stance taken by FEMA officials.

Last week, the agency's deputy administrator gave a speech which included the following. "FEMA is not a first responder. We are going to be very blunt with the American public about what FEMA can and can't do, about what the federal government can and can't do, and I hope state and local governments take this forward as well. FEMA will continue to fund the recovery for smaller disasters, but increasingly, we will be looking for state and local governments to manage those programs."

He was primarily talking about natural disasters. If municipalities are going to compare the impact of a cyber attack with that of say, a hurricane, then this would make a reliance on a federal response to events like cyber attacks on individual entities somewhat dubious.

Make no mistake there are costs. A pair of attacks in February and March of this year have so far cost the Colorado Department of Transportation an estimated $1.5 million with mitigation efforts still going on. There does not seem to be an available public assessment of the costs incurred by the City of Atlanta in response to the attack it felt. The costs involve not just those associated with technical fixes but potential revenue losses associated with delayed billings, collections, and business transactions. So what are localities doing to protect themselves?

In 2016, the International City/County Management Association (ICMA) surveyed some 3,400 municipalities in the U.S. to see what efforts were being undertaken to avoid cyber attacks. While the response rate was only 12% (who wants to admit shortcomings?), the results are nonetheless informative. Only 1% of the responding local governments have a stand-alone cybersecurity department or unit.

Most of the responding local governments do not outsource cybersecurity functions (61.8%); The inability to pay competitive salaries for cybersecurity personnel (58.3%); Insufficient number of cybersecurity staff (53.0%); and, Lack of funds (52.3%) were identified by responding local governments as severe or somewhat severe barriers to achieving the highest possible level of cybersecurity.

To the extent that this data is indicative, it is not surprising that the number of attacks and attempted attacks is rising. Yet we do not see the issue as a significant one as either a pre-sale or ongoing disclosure issue and we do not see the issue discussed on an issuer-specific basis. So we have to wonder what scale cyber attacks must reach before it becomes a significant enough credit issue?

More Bad News for Nuclear Generation

In a few states, nuclear generation operators have successfully obtained operating subsidies from states to help to justify the continued operation of generating assets in the current unregulated environment. The motivation that nuclear is a way to lower carbon dioxide emissions.

FirstEnergy Solutions (FES), its subsidiaries and FirstEnergy Nuclear Operating Company (FENOC) own, and operate two coal-fired plants, one dual fuel gas/oil plant, one pet-coke fired plant and three nuclear power plants in the competitive, or non-regulated, power-generation industry. FirstEnergy Corp. announced in November 2016 that it planned to exit the competitive generation business. On March 28, 2018, FES filed notice with PJM Interconnection LLC (PJM), the regional transmission organization, that the three nuclear facilities would be deactivated or sold during the next three years.

FirstEnergy Solutions (FES), its subsidiaries and FirstEnergy Nuclear Operating Company (FENOC) (together, the “Filing Entities”) announced that to facilitate an orderly financial restructuring, they have filed voluntary petitions under Chapter 11 of the Federal Bankruptcy Code with the U.S. Bankruptcy Court in the Northern District of Ohio in Akron. The Filing Entities collectively have over $550 million in cash, which they believe is sufficient liquidity to continue normal operations and meet post-petition obligations to employees, suppliers and customers as they come due.

The filing will allow FES to restructure its debt obligations which are estimated at some $2.1 billion of tax-exempt municipal bonds. Issues are outstanding secured under bank letters of credit and by bond insurance. The insured bonds in the amount of $427 million are insured by AMBAC. For the uninsured holders, they have lots of exposure as the debt is, as is the case with many pollution control and industrial development bonds, is unsecured. It’s amazing how many times this is overlooked by investors.

The situation shows how the power of fracking to develop natural gas resources has so significantly altered the competitive power generation landscape. There is some irony in the fact that some of these plants which are the subject of the FES filing are in the heart of Pennsylvania’s fracking region. One could argue that over some period of time, the life of these nuclear and coal generating assets was literally being sucked out from underneath them. It also highlights again the fact that fracking industry has not been taxed more efficiently by the Commonwealth of Pennsylvania, a point

we have made many times before.

Posted 04/13/2018 by Joseph Krist

Neighborly Insights

Disclaimer: Neighborly has entered into a paid agreement with Court Street Group to provide commentary on a regular basis to all customers, users, prospective customers, and prospective users of Neighborly and Neighborly Securities. The opinions and statements expressed in this report are solely those of the author(s), who is solely responsible for the accuracy and completeness of this report. The opinions and statements expressed on this report are for informational purposes only, and are not intended to provide investment advice or guidance in any way and do not represent a solicitation to buy, sell or hold any of the securities mentioned. Opinions and statements expressed reflect only the view or judgment of the author(s) at the time of publication, and are subject to change without notice. Information has been derived from sources deemed to be reliable, but the reliability of which is not guaranteed. Readers are encouraged to obtain official statements and other disclosure documents on their own and/or to consult with their own investment professional and advisors prior to making any investment decisions.

Copyright © 2026 Bond Case Briefs | bondcasebriefs.com