PNC

MUNICIPAL COMMENTARY
April 23, 2018

Tom Kozlik
215-585-1083
thomas.kozlik@pnc.com

U.S. MUNICIPAL BOND MARKET

# Cyberattacks: A Real Threat to State and Local Governments, Infrastructure

## Not Just for the Movies Anymore

In the 1983 movie release WarGames, starring Matthew Broderick and Ally Sheedy, Broderick played David, a friendly techie who spent not only hours in his room but also on-line, a very new concept in 1983. David, with his dial-up modem, connected or hacked into computers almost at will. While searching for soon to be released games he accidentally hacked into the federal government's WOPR (War Operation Plan Response) computer. David starts a game of Global Thermonuclear War with the WOPR, thinking it was a computer gaming company's system. Later, he enlists the system's designer to stop a nuclear exchange. In 1983 this topic seemed very far away from reality. Now, cyberattacks are more than movie plots and much more than just teenage kids stumbling upon a federal computer system while searching for new games to play.

*Financially motivated cyberattacks now are a notable threat.*

## Cyberattacks

Financially motivated cyberattacks now are a notable threat. This is true not just for companies, but also for municipal entities. In fact, The Multi-State Information Sharing Analysis Center notes that, "We expect that financially-motivated cyber threat activity will remain the most prevalent type of activity during 2018." In other words, we live in a much different world that we did even a few years ago. It is no coincidence that Mark Zuckerburg, the founder and current chief executive officer of Facebook spent a few days describing this new world of data collection to federal lawmakers this month. Here you can view Zuckerburg's House testimony and his Senate testimony.

What are the current leading cyber threats to state and local governments and other municipal bond issuers? Well, according to the FBI[1] they are:

- Ransomware (CryptoLocker);
- Payroll account hijacking;
- Unauthorized wire transfers;
- Internet of things (IoT) devices; and
- Insider threats

## Ransomware Attacks—A Clear and Present Danger

Cyberattacks present a clear and present danger to credit and security of state and local governments, U.S. infrastructure, and other related municipal entities. Based on recent experience, it appears the leading threat is ransomware.

What is ransomware? Ransomware, at a very basic nontechnical level, is a type of malicious software that threatens to block a victim's access to their data unless a ransom is paid.

## Examples of Recent Cyberattacks on Municipal Entities

- Atlanta is currently recovering from a March 2018 ransomware attack.[2]
- Baltimore's 911 system was breached at the end of March 2018.[3]
- Colorado Department of Transportation was targeted by ransomware for the second time at the end of February 2018.[4]

Please see analyst certification and important disclosures on page 3.

- Davidson County, NC, was attacked by ransomware in February 2018.[5]
- Mecklenburg County, NC, was attacked by ransomware in December 2017.[6]
- Portion of the U.S. power grid infrastructure was accessed in September 2017.[7]
- Sirens in Dallas, TX, were hacked and woke up residents one morning in April 2017.[8]
- The Lansing, MI, Board of Water and Power paid a $25,000 ransom after an April 2016 cyberattack.[9]

*Mecklenburg County, NC, was attacked by ransomware in December 2017.*

## Solutions to Cyberattacks

Currently the primary ways for state and local government to protect themselves against cyberattacks are:[1]

- Backing up data;
- Logging;
- Using anti-virus software;
- Applying patches;
- Isolating or segmenting critical data; and
- Using strong unique passwords.

Cyber-security-related insurance is also available from some insurance providers.

Some government entities are taking extra steps to train employees about the risks: Illinois to require cybersecurity training for all state employees. However, some experts in the field of cybersecurity believe employee cybersecurity training is not as effective as other more proactive options.[10]

*Portion of the U.S. power grid infrastructure was accessed in September 2017.*

## Outlook on Credit Landscape

We are seeing that the rating agencies are starting to ask issuers cyber-security-related questions. We also are seeing a limited amount of disclosure, usually after an attack occurs.

To date we are not aware of any municipal bond participants that have been downgraded solely as a result of a cyberattack. However, we do think state and local governments will need to take these very seriously in the future and prepare technological and procedural solutions mitigating the threat that exists from cyberattacks.

## Other sources, readings on cyber security and the U.S. Municipal Bond Market:

- Can a Cyberattack Cause a Credit Rating Downgrade? Liz Farmer; Governing; June 7, 2017.
- U.S. Muni Market Slowly Starts Paying Heed to Cyber Risks; Hilary Russ; Reuters; June 14, 2017
- Cybersecurity and Municipal Bonds: Part 1; Jim Colby; VanEck; August 16, 2017
- Cybersecurity and Municipal Bonds: Part 2; Jim Colby; Van Eck; August 24, 2017
- Cybersecurity and Municipal Bonds: Part 3; Jim Colby; Van Eck; September 12, 2017
- Cyberattacks, Like the One on CDOT, a Wakeup Call for Local Governments to Prepare; The Associated Press; March 30, 2018;
- Cyberattacks Pose a Real, If Varying, Credit Risk Across U.S. Public Finance Sectors; S&P; September 20, 2017
- Cybersecurity, Risk and Credit in Public Finance; Geoffrey Buswick; S&P; March 13, 2017
- Cyber Risk of Growing Importance to Credit Analysis; *Moody's*; November 23, 2015

*To date we are not aware of any municipal bond participants that have been downgraded solely as a result of a cyberattack.*

## Notes

[1] According to a presentation by FBI special agent Darin Murphy given to members of the Philadelphia Area Municipal Society on Thursday April 19, 2018.

[2] A Cyberattack Hobbles Atlanta, and Security Experts Shudder, Alan Blinder and Nicole Perlroth, *New York Times,* March 27, 2018.

[3] Baltimore's Emergency Call System Struck by Cyberattack, Olivia Beavers, *The Hill,* March 28, 2018.

[4] Ransomware Strikes CDOT for Second Time Even as Agency Still Recovering from First SamSam Attack, Tamara Chuang, *The Denver Post,* March 1, 2018.

[5] North Carolina County Announces Full Recovery from Ransomware Attack, Ben Coley, *Government Technology,* March 20, 2018.

[6] Fake Email, Stolen Log-Ins Opened Door to Widespread Hack on Mecklenburg County, Anna Douglas, *Charlotte Observer,* December 12, 2017.

[7] Hackers Gain Direct Access to U.S. Power Grid Controls, Andy Greenburg, *Wired,* September 6, 2017.

[8] Hacking Attack Woke Up Dallas with Emergency Sirens Officials Say, Eli Rosenberg and Maya Salam, *The New York Times,* April 8, 2017.

[9] Lansing Utility Paid $25,000 Ransom after Cyberattack, Ken Palmer, *Lansing State Journal*, November 9, 2016.

[10] Please see comments by Area 1 Security CEO Oren Falkowitz in Want to Prevent Cyberattacks? Don't Count on Employee Training to Stop Them; Katherine Barrett and Richard Greene; Governing; April 19, 2018.