VanEck® VECTORS

Cybersecurity and Municipal Bonds: What is at Stake?

By James Colby, Portfolio Manager and Senior Municipal Strategist and Tom Butcher, Communications

Jim Colby, Municipal Bond ETF Portfolio Manager at VanEck, and Tom Butcher, VanEck Communications, explore the intersection between cybersecurity and the municipal bond market. This paper is also available to the public as a three part series on our website: Cybersecurity and Municipal Bonds.

Cybersecurity Challenges Impact Government: At Federal, State, and Local Levels

The importance of cybersecurity has never been more apparent. Cybersecurity issues are a growing challenge that impact many aspects of our economy, including most of the services provided by municipal borrowers.

Although not readily obvious, municipal services are vital to the smooth running of daily life. These services run the gamut, including funding and managing traffic lights, supplying electric and sewer services, water supply, maintaining/building roads, building bridges, supervising elections, running hospitals, and providing mental and physical health support.

Safeguarding municipal services is vital at all levels: federal, state, and local. Both government and the private sector are spearheading important security initiatives to meet the growing cybersecurity challenges that are involved.

Municipal Services Impact Everyday Life

Municipal governments are involved in most aspects of our lives, and each service provided is subject to unique cybersecurity issues.

Here is just one example. Municipal governments collect (and need to "safeguard") a tremendous amount of information – any or all possibly containing personally identifiable information (PII) or sensitive personal information (SPI) – including, of course, Social Security numbers. Examples of how this information is collected include house deeds, mortgage documents, records of births, marriages, deaths, medical records, driver licenses, and court documents (e.g., divorce settlements).

Both PII and SPI are subject to the impacts of cybersecurity personal identity theft, and awareness of identity and access management (IAM) is playing an evolving role in tightening cybersecurity frameworks in both the public and private sectors.

Examples: Federal Cybersecurity Incidents

Each year, in a report to Congress, the Office of Management and Budget (OMB) provides "summary information on the number of cybersecurity incidents that occurred across the government and at each Federal agency."[1] These incidents are notable not only for their number, but also for their variety, as shown in the following table.

Federal Agency Reported Incidents by Attack Vector – Fiscal Year 2016

Attack Vector	Description	CFO*	Non-CFO*	Gov't-wide
Attrition	Employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	108	1	109
E-mail/Phishing	An attack executed via an email message or attachment.	3,160	132	3,292
External/Removable Media	An attack executed from removable media or a peripheral device.	132	6	138
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	60	4	64
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	3,920	210	4,130
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	5,313	377	5,690
Web	An attack executed from a website or web-based application.	4,766	102	4,868
Other	An attack method does not fit into any other vector or the cause of attack is unidentified.	11,365	437	11,802
Multiple Attack Vectors	An attack that uses two or more of the above vectors in combination.	789	17	806
Total		**29,613**	**1,286**	**30,899**

Source: FISMA FY 2016 Annual Report to Congress.

** Chief Financial Officers Act agencies are those agencies designated in the CFO Act (with the addition of Department of Homeland Security and minus the Federal Emergency Management Agency). In practice, the CFO Act agencies are the 24 largest Federal agencies in terms of budget; the 23 civilian CFO Act agencies are the CFO Act agencies minus the Department of Defense.*

Examples: Municipal Cybersecurity Incidents

The breadth of cybersecurity incidents that can impact municipalities is deep and wide. The following are a sample of notable cybersecurity incidents that have impacted the municipal space over the past several years.

Personal Information

October 2014 – Personal information, including Social Security numbers, of more than 850,000 people possibly compromised when hackers gain access to Oregon Employment Department database.[2]

February 2016 – Hollywood Presbyterian Medical Center pays 40 bitcoin (around $17,000) to hacker who "seized control of the hospital's computer systems and would give back access only when the money was paid."[3]

Services

August 2003 – On August 14, 2003, nearly 14 years ago, millions of people in both Canada and the U.S. were hit by the great Northeast blackout caused primarily by a software bug. There was no power to run the trains, and no power for pumping domestic fresh water, treating raw sewage, running lighting, refrigerators, and air conditioning, filling up with gasoline, accessing electronic airline tickets, running cable TV, and recharging cell phones. This situation was caused by a software accident, and not a breach cybersecurity, but its impact was enormous.

Fast forward to 2015 in Ukraine.

December 2015 – It was certainly no accident on December 23, 2015, when malicious hackers deprived some 230,000 people in the Ivano-Frankivsk region of West Ukraine of power for up to six hours. The power company Prykarpattyaoblenergo's control center had fallen victim to a sophisticated cyberattack.

Although this happened many thousands of miles away, according to one article: "the control systems in Ukraine were surprisingly more secure than some in the U.S."[4] Should a future power grid cyberattack occur in the U.S., the impacts could be enormous. While the event in Ukraine may have affected only 230,000 people, the Northeast blackout of 2003 was estimated to have affected at least 55 million people in both Canada and the U.S. Eleven people died.[5]

March 2016 – The U.S. Justice Department indicted seven Iranians not only for cyberattacks on a number of American banks, but also for trying to take over the controls of a small suburban dam in Rye, New York.[6]

September 2017 – On September 6, 2017, security firm Symantec reported[7] that dozens of energy companies, including in the U.S., had been subject to hacker attacks in spring and summer this year. The firm's analysis found that "hackers obtained what they [power firms] call operational access … giving them the ability to stop the flow of electricity into U.S. homes and businesses." According to an article on the attacks in WIRED,[8] Symantec noted that hackers had never before "been shown to have that level of control of American power company systems."

Addressing Cybersecurity Issues

For some years now, initiatives have existed both to "enhance the security and resilience of the Nation's critical infrastructure"[9] and provide "timely and actionable information" to "state, local and territorial (SLTT) governments."[10]

Critical Infrastructure Sectors[9]	
Chemical	Financial Services
Commercial Facilities	Food and Agriculture
Communications	Government Facilities
Critical Manufacturing	Healthcare & Public Health
Dams	Information Technology
Defense Industrial Base	Nuclear Reactors, Materials, and Waste
Emergency Services	Transportation Systems
Energy	Water and Wastewater Systems

Creation of the NIST Cybersecurity Framework under Obama

Cybersecurity's importance is being recognized at the highest levels. Help from our central government in Washington DC in tackling cybersecurity issues has been available to state and local governments (and others) for some time.

On February 12, 2013, President Barack Obama issued the first executive order addressing cybersecurity: Executive Order (EO) 13636 entitled "Improving Critical Infrastructure Cybersecurity". The order directed the Executive Branch to "enhance the security and resilience of the Nation's critical infrastructure".[11]

One of the most important things resulting from EO 13636 has been the "Framework for Improving Critical Infrastructure Cybersecurity"[12] developed by the National Institute of Standards and Technology's (NIST). The NIST Cybersecurity Framework follows a set of industry standards and best practices to help organizations manage cybersecurity risks, and was established through the collaboration of the government and the private sector.

NIST Cybersecurity Framework Becomes Policy under Trump

President Trump recognized the importance of standardizing cybersecurity practices by issuing EO 13800[13] on May 11, 2017. This EO turned the NIST framework into federal government policy that requires NIST to provide cybersecurity process frameworks for all federal agencies.[14]

NIST highlights the fact that cybersecurity cannot be addressed by technology alone. The NIST Cybersecurity Framework goes beyond technology and also addresses both people and processes. All are critical to solving cybersecurity issues. Just as importantly, whatever an organization's size, the degree of its exposure to cybersecurity risk, or its cybersecurity sophistication, the NIST framework can help it "to apply the principles and best practices of risk management."[15]

How Municipalities Benefit from NIST Framework

The NIST Cybersecurity Framework provides an important resource for municipal governments. State and local governments "face unique challenges due to limited resources, complex regulations, and an increasingly sophisticated threat environment,"[16] according to global tech giant Cisco. The NIST Framework offers municipalities a proven risk-based approach to tackling cyberthreats, one that "reduces complexity and provides visibility, continuous control, and advanced threat protection across the extended network and attack continuum before, during, and after a cyberattack."[17]

US-CERT: A Safer, Stronger Internet for All Americans

Cybersecurity help is also available to state and local municipalities through US-CERT (the U.S. Computer Emergency Readiness Team), established in 2003. Its overall mission is to strive for "a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world." One of US-CERT's critical mission activities is to provide timely and actionable cybersecurity information to state and local governments.

Possible Drivers to Action

Whether private or public, organizations need incentives to address cybersecurity. Come the day of reckoning when an organization/local or state government is held to cybersecurity ransom, any excuses will likely be recognized as hollow.

The Risk of Cyberattack

We are all potentially at risk of cyberattack – directly or indirectly. When it comes to municipalities, this may not always be obvious to the average state or city taxpayer. However, it does not even seem to be that obvious to, or maybe even much appreciated by, many municipalities and/or states.

Even with resources like the NIST Framework and US-CERT available to them, governments and administrations appear to be moving slowly to protect themselves from cyberattacks – whether targeted at the sensitive information they hold or the services for which they are responsible. If they are actually doing anything, it is not readily evident. You would have thought that, at the very least, they would be telling taxpayers that they are "on it".

Some investors may gain a modicum of comfort from the news that, despite the manifest dysfunctionality of its government in Springfield, the state of Illinois is now adopting mandatory cybersecurity awareness training for all state employees.[18] It appears that Illinois is only the 15th state to require such training: What about the other 35?

What Is There To Be Done About It?

Addressing cybersecurity successfully will be predicated on a significant psychological shift in thinking. A shift to thinking first and foremost about prevention, not cure. As cybersecurity expert Hans Holmer[19] described it to me the other day "…by externalizing the responsibility associated with cybersecurity, those who are vulnerable willfully ignore the fact that their security essentially boils down to just what they are happy to let the intruders/thieves/hackers… do".

There are many different ways nefarious intruders can be slowed down, the impact minimized, and the cost reduced. But it all has to be done with front-end protection. Think of it as akin to donning a crash helmet before riding a motorcycle.

All a Matter of Incentive

In my view, the real key to success is incentivizing people to establish cybersecurity and to maintain it effectively. The difficulty lies in determining just what that incentive should be. Protection of property and essential services is a universal need, but urgency is still lacking.

Possible Drivers to Action

One possible driver to action could simply be alerting the public through their local media outlets just what havoc can be, and has been, wrought by cyberattacks. For example, at the National Health Service in the U.K. and the power company Prykarpattyaoblenergo in Ukraine. While the latter appears to have been a targeted attack, the former was simply about money. While both were malicious and extremely damaging, they could also be viewed simply as warning shots and indicative of what further might happen.

Another driver could lie with municipalities' furthering their own commitments to high-quality and reliable public services. Terry Smith, CEO and founder of Smith's Cyber Security Gradings, believes that with the tradition of first-class service to uphold, public sector (both state and local) cybersecurity professionals are willing to meet the challenge, but the critical physical infrastructure is weak.

I believe two other potentially effective approaches (if they were adopted) lie with the muni bond market itself. First, lenders should insist that bond issuers meet certain minimum standards of cybersecurity. These could be based on guidelines and standards set out by NIST and/or US-CERT. And their adherence to these standards will be monitored on a continuing basis.

A commitment to, and the subsequent maintenance of, these standards would be incorporated in municipal bond offering documents; that is, a clause covering cybersecurity would become standard. Its absence would likely result in a yield penalty to the issuer similar to what occurs with bond insurance.

In the second instance, a commitment to and the recognition of standards by, credit rating agencies would have a direct bearing on an issuer's ability to obtain a stronger rating for the bond: the tradability of the bond would likely improve as a result. Cybersecurity gradings do already exist in the private sector, but not yet in the muni space.

Conclusion: Cybersecurity Standards that Safeguard Municipal Lenders are Critical

The services provided by municipal borrowers have always been, and remain, vital to our everyday life. The need to protect these services from possible disruption has become ever more important. Cybersecurity can help provide this protection. Cure, as opposed to prevention, is less and less an acceptable option. Luckily, initiatives such as those from NIST and US-CERT already exist. These have been designed to help all levels of government address the challenges of cybersecurity. Incentive remains the key issue.

In sum, initiatives from analysts, bankers, and legal teams, in concert with issuers, to establish a standard clause in bond offering documents committing the borrower to establish and maintain certain cybersecurity standards are of paramount importance. Further, tying an issuer's credit rating to a commitment to, and subsequent maintenance of, certain cybersecurity standards needs the attention of credit rating agencies to provide the market incentive (lower cost) the issuers seek.

[1] The Office of Management and Budget: Federal Information Security Modernization Act of 2014 - Annual Report to Congress: Fiscal Year 2016

[2] Oregon Live: Employment Department data breach: more than 851,000 people could be at risk, October 13, 2014

[3] Los Angeles Times: Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating, February 18, 2016

[4] Wired: INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID, March 3, 2016

[5] Electric Light & Power: 13 Years After: The Northeast Blackout of 2003 Changed Grid Industry, Still Causes Fear for Future, August 23, 2016

[6] The New York Times: U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam, March 24, 2016

[7] Symantec: Dragonfly: Western energy sector targeted by sophisticated attack group, September 6, 2017

[8] WIRED: Hackers Gain Direct Access to US Power Grid Controls, September 6, 2017

[9] The White House, Office of the Press Secretary: Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013

[10] https://www.us-cert.gov/about-us

[11] The White House, Office of the Press Secretary: Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013

[12] National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1., January 10, 2017

[13] The White House, Office of the Press Secretary: STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE, May 11, 2017

[14] GovCon Wire: Trump Orders All Federal Agencies to Provide Cyber-Security Plans to NIST Within 90 Days, May 12, 2017

[15] National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1., January 10, 2017

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Management Strategy • Supply Chain Risk Management	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

Source: National Institute of Standards and Technology.

[16] Cisco and The Chertoff Group: Addressing Critical Infrastructure Cyber Threats for State and Local Governments – Application of a Threat-Centric Approach through the NIST Cybersecurity Framework, 2015

[17] Ibid.

[18] The Hill: Illinois to require cybersecurity training for all state employees, August 8, 2017.

[19] Hans Holmer is a senior cyber strategist. He has more than 30 years of experience in cybersecurity, human intelligence, and counterintelligence in the United States and overseas. Mr. Holmer served as a case officer for the Central Intelligence Agency (CIA) for over 25 years where he assessed vulnerability and detected threats to internal and external network and infrastructure.

IMPORTANT MUNI NATION® DISCLOSURE

This content is published in the United States for residents of specified countries. Investors are subject to securities and tax regulations within their applicable jurisdictions that are not addressed in this content. Nothing in this content should be considered a solicitation to buy or an offer to sell shares of any investment in any jurisdiction where the offer or solicitation would be unlawful under the securities laws of such jurisdiction, nor is it intended as investment, tax, financial, or legal advice. Investors should seek such professional advice for their particular situation and jurisdiction.

VanEck does not provide tax, legal or accounting advice. Investors should discuss their individual circumstances with appropriate professionals before making any decisions. This information should not be construed as sales or marketing material or an offer or solicitation for the purchase or sale of any financial instrument, product or service.

Please note that MUNI NATION® represents the opinions of the author and these opinions may change at any time and from time to time. Not intended to be a forecast of future events, a guarantee of future results or investment advice. Current market conditions may not continue. Non-VanEck proprietary information contained herein has been obtained from sources believed to be reliable, but not guaranteed. No part of this material may be reproduced in any form, or referred to in any other publication, without express written permission of VanEck. MUNI NATION is a trademark of Van Eck Associates Corporation.

All indices listed are unmanaged indices and do not reflect the payment of transaction costs, advisory fees or expenses that are associated with an investment in a fund. An index's performance is not illustrative of a fund's performance. Indices are not securities in which investments can be made.

Municipal bonds are subject to risks related to litigation, legislation, political change, conditions in underlying sectors or in local business communities and economies, bankruptcy or other changes in the issuer's financial condition, and/or the discontinuance of taxes supporting the project or assets or the inability to collect revenues for the project or from the assets. Additional risks include credit, interest rate, call, reinvestment, tax, market and lease obligation risk. High-yield municipal bonds are subject to greater risk of loss of income and principal than higher-rated securities, and are likely to be more sensitive to adverse economic changes or individual municipal developments than those of higher-rated securities. Municipal bonds may be less liquid than taxable bonds.

The income generated from some types of municipal bonds may be subject to state and local taxes as well as to federal taxes on capital gains and may also be subject to alternative minimum tax.

Diversification does not assure a profit or protect against loss.

Investing involves substantial risk and high volatility, including possible loss of principal. Bonds and bond funds will decrease in value as interest rates rise. An investor should consider the investment objective, risks, charges and expenses of a fund carefully before investing. To obtain a prospectus and summary prospectus which contain this and other information, call 800.826.2333 or visit vaneck.com. Please read the prospectus and summary prospectus carefully before investing.

VanEck®

Van Eck Securities Corporation, Distributor
666 Third Avenue | New York, NY 10017
vaneck.com | 800.826.2333