HilltopSecurities
A Hilltop Holdings Company

Importance of Cybersecurity to Government and Infrastructure Assets Continues

Threat of Cyber, Ransomware Attacks Remains

Tom Kozlik
Head of Municipal Strategy & Credit
214.859.9439
tom.kozlik@hilltopsecurities.com

A Risk to be Taken Seriously

In the past, it was assumed that only individuals and corporations—and for that matter mostly just larger international companies—were at risk for cyberattacks. Individuals have fallen victim, as we have seen from time to time, to credit card infiltrations. And companies have been targets because they possess business development, industry secrets, or other innovations they wanted to keep hidden from competitors or other intruders. But, the threat from cyberattacks is no longer just a matter of high-level corporate or international government espionage. Cybersecurity is—and is expected to remain—a concern for U.S. state and local governments, education institutions, health care providers, and other infrastructure assets.

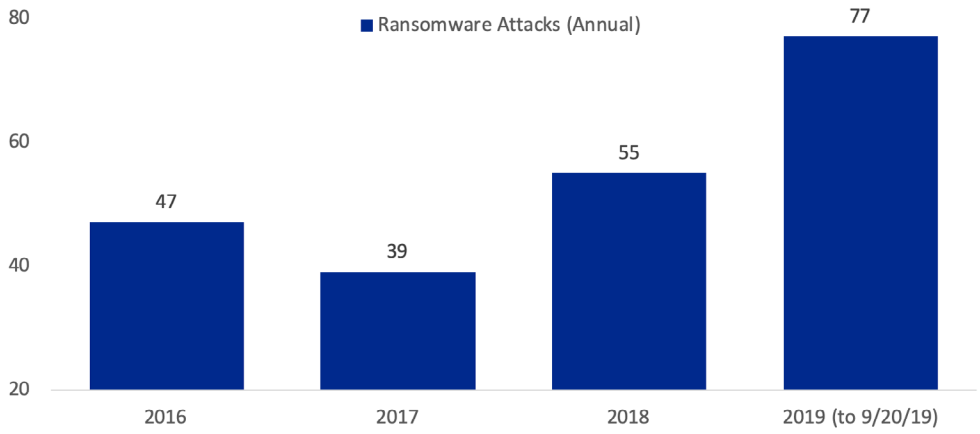
We are seeing situations where the results of attacks are impacting municipal issuer credit quality. S&P lowered the outlook on Princeton Community Hospital (BBB+) in West Virginia to "Negative" in April this year because of a ransomware attack that cost $10.8 million, per management's estimates.

We are seeing situations where the results of attacks are impacting municipal issuer credit quality.

How Do Hackers Gain Access?

For most people, computer passwords are an afterthought at best and more commonly seen as a nuisance. Some try to incorporate personal aspects into their passwords in order to remember them. In Texas, a common computer password could be "Cowboys21," for example. In the Seattle area, "Seahawks12" is the most common. For music fans, "blink182" and "50cent" are commonly assigned by users. And the thoughtless "123456" remains frequently utilized as well.[1] Hackers are on to the use of these common passwords.

Number of Ransomware Attacks on U.S. State & Local Governments



Source: Recorded Future and HilltopSecurities.[2]

Please see analyst certifications and disclosure starting on page 3.

It is not as hard to access computer systems as one might think. This is why government (and company) Information Technology (IT) departments have upped their cyber defense and surveillance efforts in recent years. And whether hackers guess, possess a program that uncovers your password, or gain access via a seemingly harmless link for an on-sale blouse or a video game cheat code, the cyber environment should not be considered fully safe or forgiving.

If you think you see more articles about cyberattacks related to state and local government and other municipal entities, it is because these security breaches are happening more often.

Make No Mistake, Cyberattacks are Occurring More Often

If you think you see more articles about cyberattacks related to state and local government and other municipal entities, it is because these security breaches are happening more often. The most common type of cyberattack on governments so far have been ransomware attacks. Ransomware is malicious software purposefully designed to infiltrate a victim's computer or network and restricts users from accessing their computers or valuable data stored in their memory or network files. User access to the computers and/or the data remains restricted until the victim pays the attacker whatever ransom is demanded.

Variety of Cybersecurity Threats

While ransomware is the most common technique cyber attackers use, it's not the only one. So, what exactly are the leading cybersecurity threats for state and local governments, non-profits, and other related organizations? According to the FBI[3] they are:

The most common type of cyberattack on governments so far have been ransomware attacks. Ransomware is malicious software purposefully designed to infiltrate a victim's computer or network and restricts users from accessing their computers or valuable data stored in their memory or network files.

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

Recent Government Cyberattacks

This month, a recent high profile attack occurred in Oklahoma where hackers stole $4.2 million from the law enforcement retirement system.[4] The August 2019 attack on 22 local government agencies in Texas made national headlines.[5] But, this attack was not important just because small governments were the target. There was also a technical reason it was important. It was the first time that a different, sophisticated level of ransomware was used on local governments. When asked at an industry conference if such an attack was likely to occur again an industry expert responded:

> "Will it happen again? It is happening again. It's probably happening right now," said James Globe, vice president of operations for the Center for Internet Security's Multi-State Information Sharing and Analysis Center.[6]

Armor, a security solutions provider, also identified 49 education institutions, which include higher-ed institutions and local school districts that have been impacted by cyberattacks since January 2019, according to recent data.[7]

This month, a recent high profile attack occurred in Oklahoma where hackers stole $4.2 million from the law enforcement retirement system.

Potential for Aid from Federal Government

The State and Local Government Cybersecurity Act, proposed in the Senate, is expected to be considered by lawmakers this fall. The act has already received a rare endorsement by the National Association of Chief Information Officers, and was approved by the Homeland Security and Governmental Affairs Committee this summer.[8] The legislation seeks to create a new grant program housed in the Department of Homeland Security for state and local governments. There are also several other pieces of legislation that in some way, shape, or form could benefit municipal issuers, governments, non-profits, and infrastructure projects if they become law.[9]

[1] *See more here for common passwords: If One of these 100,000 Passwords is Yours, Change It; by Travis Pittman; WFAA.com; April 24, 2019.*
[2] *Recorded Data's information access in Ben Miller's article in Government Technology, Hackers Are Hitting Government More, but That's Nothing New; September 23, 2019.*
[3] *According to a presentation by FBI special agent Darin Murphy given to members of the Philadelphia Area Municipal Society on Thursday April 19, 2018.*
[4] *Vizcaino, Maria Elena; Oklahoma Pension Fund Cyber Attack Shows Risk for Munis; Bloomberg; Sept 13, 2019.*
[5] *Collier, Kevin; Texas Working to Recover From Ransomware Attack on 22 Government Targets; CNN; Aug 20, 2019.*
[6] *Wood, Colin; Expect More Sophisticated Ransomware Attacks Like Texas, Expert Says; StateScoop; Aug 20, 2019.*
[7] *Armor Identifies 10 Ransomware Victims in the Past 9 Days, All of Them Educational Institutions. Includes lists.*
[8] *Freed, Benjamin; Congress Moving Closer Toward Cybersecurity Aid to State and Local Governments; StateScoop; Sept 23, 2019.*
[9] *Please see Cynthia Brumfield's The Cybersecurity Legislation Agenda: 5 Areas to Watch; CSO Online; Feb 21, 2019.*