Importance of Cybersecurity to Government and Infrastructure Assets Continues

Threat of Cyber, Ransomware Attacks Remains

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.

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

![Ransomware Attacks Chart](chart_url)

Source: Recorded Future and HilltopSecurities.2
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.

### 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, they are:

- 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. The August 2019 attack on 22 local government agencies in Texas made national headlines. 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.

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.

### 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. 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.
The paper/commentary was prepared by Hilltop Securities (HTS) and Hilltop Securities Asset Management (HSAM). It is intended for informational purposes only and does not constitute legal or investment advice, nor is it an offer or a solicitation of an offer to buy or sell any investment or other specific product. Information provided in this paper was obtained from sources that are believed to be reliable; however, it is not guaranteed to be correct, complete, or current, and is not intended to imply or establish standards of care applicable to any attorney or advisor in any particular circumstances. The statements within constitute the views of HTS and/or HSAM as of the date of the document and may differ from the views of other divisions/departments of affiliate Hilltop Securities Inc. In addition, the views are subject to change without notice. This paper represents historical information only and is not an indication of future performance. This material has not been prepared in accordance with the guidelines or requirements to promote investment research, it is not a research report and is not intended as such.

Hilltop Securities Asset Management is an SEC-registered investment advisor. Hilltop Securities Inc. is a registered broker-dealer, registered investment adviser and municipal advisor firm that does not provide tax or legal advice. HTS and HSAM are wholly owned subsidiaries of Hilltop Holdings, Inc. (NYSE: HTH) located at 1201 Elm Street, Suite 3500, Dallas, Texas 75270, (214) 859-1800. Member: NYSE/FINRA/SIPC.

© 2019 Hilltop Securities Inc. | All rights reserved MEMBER: NYSE/FINRA/SIPC | HTS371752370