Bond Case Briefs

Municipal Finance Law Since 1971

Hacking Threat Comes Into Focus for Municipal Finance.

As computer hackers become more creative in their attacks on government enterprises, different segments of the municipal industry are being forced to react.

“Everyone saw what happened in Atlanta and thinks that could be us,” said Richard Lllewellyn, Los Angeles’ chief administrative officer.

In late March, a hacking crew calling itself the SamSam Group froze a wide range of Atlanta city systems for five days and demanded a ransom equal to $51,000 in bitcoin. The hackers snarled a broad range of online systems, forcing city workers to swap electronic systems for paper, with computers rendered useless while the city worked for five days to restore service.

The Atlanta hack spared the 911 system, but the story was different in Baltimore, where the automatic dispatch system at the 911 center was shut down for an entire Sunday in March while technicians worked to restore a server breached by hackers.

Colorado’s Department of Transportation was recovering from a February attack that froze 2,000 computers when the system became re-infected. The hack, considered a variation of the SamSam ransomware that struck Atlanta, locked computer files and demanded a ransom for their safe return.

Conversations with S&P Global Ratings analysts and an FBI agent made Tom Kozlik, a PNC Bank credit analyst, realize “there isn’t much the FBI or other authorities can do to stop those kinds of ransomware attacks.”

The issue has become so commonplace that municipalities are being advised to describe the risks in bond offering documents.

Los Angeles Mayor Eric Garcetti launched the LA CyberLab in August to share information about cybersecurity threats with businesses in the city. The lab, a public-private partnership, helps to thwart cyber criminals by disseminating information and intelligence based on the analysis of more than one billion security-related events and over four million attempted intrusions into city networks per day, according to the mayor’s office.

The problem has struck close to home; the Port of Los Angeles’ largest terminal was closed for several days in 2017 when the NotPetya computer worm struck shipping firm Maersk, slowing its computers’ functions to a crawl.

In February, a Houston man was indicted on charges of using the Los Angeles Superior Court system to send phishing emails to direct people to a fake American Express website.

Earlier, Garcetti spent federal funds on efforts like installing Splunk, data management software that centralizes cybersecurity monitoring.

New York Mayor Bill de Blasio announced last week the city would add $41 million to its fiscal 2019 budget for cyber security projects.

De Blasio pointed to the attack on the United Kingdom's National Health Service, where medical personnel could not access patient records, putting lives at risk.

Cities have to weigh the cost of the ransom against the millions it would cost to fix systems that were electronically torched by cyber criminals.

Colorado didn't pay a ransom, but Atlanta did.

The FBI's advice runs counter to the popular belief perpetuated by movies where authorities instruct victims against ransom payments, Kozlik said.

When FBI special agent Darin Murphy gave a presentation to members of the Philadelphia Area Municipal Society in April, he told them that it was a business decision for each government, Kozlik said.

A city has to weigh paying something like a $25,000 ransom versus millions of dollars to repair a corrupted computer system and losing revenue while the system is down, Kozlik said.

Kozlik issued a commentary on the subject in April, and plans to spend the next few months analyzing the threats to municipal credits to offer more detailed guidance.

Orrick, Herrington & Sutcliffe advises clients in nearly every case to include information about cyber security in bond offering documents, said Roger Davis, co-chair of the firm's public finance department.

"It might be a separate section, or it might just be a risk factor, but almost all of the transactions I can think of lately have included some disclosure or advice on cyber security," Davis said.

He said it has been at least a year and a half since Orrick began including information in bond documents.

California had one of the largest examples of a municipal market data breach in 2015, when hackers broke into the UCLA hospital network accessing the records of 4.5 million people. UCLA's hospital network includes four hospitals and 150 offices across southern California.

The trigger for S&P to begin considering the potential credit risk for muni credits came after South Carolina's tax filings were hit in 2015, said Geoff Buswick, an analyst. The amount of taxes paid or returns received were posted to an email group, Buswick said.

Since then, it has become more common to see such online crime happen to cities and school districts, Buswick said.

S&P pulled a group together in January 2017 to draft a reference guide on potential credit risks from cyber attacks, Buswick said.

The analysts looked at what the federal government was advising state and local governments, and the guidelines laid out by the Multi-State Information Sharing and Analysis Center of the Center for Internet Security, a non-profit entity that coordinates the IT industry to safeguard private and public organizations.

S&P has not created a separate criteria for evaluating municipal cyber risk, but advises analysts to start asking municipalities questions about their defenses and how prepared they are in the event an attack occurs. Many of the questions fall under the analysis of how well a municipality is managed.

S&P also asks if a municipality has insurance coverage.

S&P has yet to downgrade any municipal credit because of cyber risk, but Buswick said what happened to Lansing, Michigan is a good example of how these attacks can act as a stress test of sorts and reveal other weaknesses.

The Lansing Board of Water & Light paid the ransom of $25,000. It was insured, but when its system was attacked officials decided it was too vulnerable and replaced it at a cost of $2 million, Buswick said. The $800,000 in insurance did not cover that expense. If the city had been facing a liquidity crunch and it had not been able to cover the additional $1.2 million expense, its ratings could have been impacted, Buswick said.

In Atlanta, residents still can't pay their water bills online, Buswick said. In that attack, he said, the hackers tried every possible combination of password they could until they could get in.

Georgia has a strong system and has worked with Atlanta on protecting its computer network.

"They have done best practices to try to protect themselves, but attackers are getting more sophisticated," he said.

Moody's Investors Service views "cyber risk as event risk – an incident with a low probability, but potentially high impact," said Joe Mielenhausen, a spokesman.

"Our fundamental credit analysis for municipalities incorporates numerous stress tests, and a cyber event could trigger one of those stress scenarios," Mielenhausen said. "Cyber attacks can shut down service and increase near-term costs for local governments, but ultimately they are manageable assuming the government has ample liquidity and other preparation measures in place."

Aravind Swaminathan, a partner in Orrick's Seattle office, said cities have to maintain ongoing surveillance, because as soon as they overcome one tactic hackers find another method of access.

Swaminathan, a prosecutor in the Department of Justice's computer hacking and intellectual property section for six years before joining Orrick, works with Davis in guiding clients on more than bond disclosure. He is also co-chair of the firm's cyber, privacy and data innovation group.

Municipalities that are not public finance clients are turning to the firm for help in creating a defense system against hackers, meeting federal guidelines on such systems, and determining the best way to handle a data security incident, Swaminathan said.

The team also aids clients if they are facing regulatory or class action lawsuits when protections fail.

"Our practice has handled 350 data security incidents in the past four years," he said. He did not know what percentage were municipal versus private industry breaches.

"This is a world that is bound only by the creativity of the bad guy, which seems to be limitless," Swaminathan said. "We are becoming more aware, but the bad guys are evolving just as we are."

Paul Burton contributed to this report.

The Bond Buyer

By Keeley Webster

May 03 2018