Bond Case Briefs

Municipal Finance Law Since 1971

Cyber Vulnerabilities Could Impact Municipal Finance.

Municipal bond credit analysts consider governments unprepared for cyberattacks, a recent survey says.

While cybersecurity risk management has long been on the radar of government IT managers, it's also attracting the attention of municipal finance organizations.

In a Dec. 14 survey by Hilltop Securities, municipal bond credit analysts said they felt state and local governments were unprepared for cyberattacks. A full 63% said they thought governments were "hardly prepared" for cyberattacks, and 30% said they were "somewhat prepared." Only 6% considered state and local governments "on the way to being prepared, with none of the analysts considering municipalities "very prepared" or even "prepared."

The growing number of ransomware attacks state and local governments are facing has municipal bond issuers on alert. The ransomware attack on Atlanta was a "watershed moment," Omid Rahmani, associate director for U.S. public finance at Fitch Ratings, said in a Nov. 1 interview with Hilltop.

In March 2018, Atlanta was hit with SamSam ransomware that crippled the city's online systems and brought many city services to a grinding halt. The hackers demanded $51,000 worth of bitcoin, which the city refused to pay. Estimates of the ultimate recovery cost approached $17 million.

One of changes since the Atlanta attack, according to Rahmani, is that hackers are no longer using shotgun style attacks where they target a large number of entities and hope one or two of them engages the malware. Now, they are analyzing municipal disclosure documents to find not only potential cyber vulnerabilities but also determining a city's "actual appetite for payment," he said.

The recent breach of the Kronos Cloud Solution platform that many municipalities and health care organizations rely on for payroll and workforce tracking is another attack vector agencies must manage and that finance organizations take into consideration.

These vulnerabilities have driven up premiums for cyber insurance. While nearly 90% of local governments surveyed by Public Technology Institute said they have cyber insurance, up from 78% in 2020, policies are increasingly complex and require agencies to meet stringent cybersecurity controls.

Public sector entities with legacy systems and under-resourced IT departments may find it harder to find affordable coverage – especially as ransomware attackers demand larger payoffs. Those with inadequate coverage could face even "greater financial and reputational risks from cyberattacks, which could have negative credit implications, according to Fitch Ratings.

"The landscape is changing quite rapidly right now, from the cybersecurity insurance and the threat landscape side, which leaves local governments in the middle dealing with issues they traditionally haven't had to deal with," Rahmani told The Record.

gcn.com

By Susan Miller

JANUARY 3, 2022 03:54 PM ET