Bond Case Briefs

Municipal Finance Law Since 1971

Cyberattack Hobbles Baltimore for Two Weeks and Counting.

City faces second ransomware attack in 15 months; water bills, home sales face delays

BALTIMORE—About 10,000 city government computers here remain frozen two weeks after a disruptive cyberattack that has delayed home sales and halted water bills.

Baltimore was hit May 7 by hackers demanding an undisclosed sum to unlock computers. The city hasn't paid, and the Federal Bureau of Investigation is probing the incident. Mayor Bernard C. "Jack" Young has warned it could take months to recover some systems.

"It's extremely alarming," said City Council President Brandon Scott.

This is Baltimore's second cyberattack in 15 months. In March 2018, a short-lived ransomware attack on the city's 911 system forced dispatchers to temporarily relay addresses and other information to first-responders by phone rather than electronically.

City officials emphasized that key services such as 911 emergency dispatch haven't been affected by the current cyberattack.

Ransomware attacks are common in both the public and private sectors, and attackers are generally looking to exploit any vulnerability they can turn into extortion for money. After accessing systems through methods like malicious emails, hackers can encrypt files and then demand payment in bitcoin to unlock them.

Local governments are often more vulnerable than private companies, said Bill Siegel, chief executive at Coveware, a Connecticut-based firm that helps entities victimized by cyberattacks. "I think broadly they are not prepared for these sorts of things, they do not have the budget," he said.

For Baltimore, "I think it's pretty obvious that they have not been able to stay ahead of it," said Mr. Siegel, who hasn't worked with the city on this problem.

Frank Johnson, Baltimore's chief information officer, didn't respond to a request to comment Tuesday.

Mr. Scott said he will form a special committee to investigate the episode and city officials' handling of it, "but most importantly, how they're going to work to have this not happen in the future."

While the city and outside contractors continued working Monday to restore the municipal computer system, officials began implementing a workaround to allow home sales to proceed.

Between 200 and 300 closings have been hung up because the city couldn't tell title insurers whether the seller had any unpaid liens, said Alan Ingraham, chief executive of the Greater Baltimore Board of Realtors.

Starting Monday, sellers were able to sign an affidavit promising to pay any liens, such as unpaid water bills, that are discovered once the computers come back online. Mr. Young's office said the city processed 42 applications for property deeds on the first day of the workaround.

Mark Glazer, executive director of the Maryland Land Title Association, a trade group for title insurers and agents, said this helps but he hopes the city resumes full operations quickly. May and June are busy months for deal closings, he said.

Meanwhile, the problems continue for some city agencies. Epidemiologists in Baltimore's health department can't access the state network that helps them warn the public when bad batches of street drugs trigger overdoses. And the city's public-works department can't generate new water bills for customers, which could mean residents will get unusually high bills once the problem is fixed.

"We can't see the consumption data that our meters are collecting and sending to us," said Jeff Raymond, a spokesman for the public-works department.

Greenville, N.C., was attacked last month by the same type of ransomware afflicting Baltimore, dubbed Robbinhood. The attackers demanded 13 bitcoins—worth roughly $69,000 at that point—to unlock the city's files. The city didn't pay, spokesman Brock Letchworth said in an email.

"While not 100% restored, all of our major technology needs are now being met," he said.

Atlanta last year endured one of the highest-profile ransomware attacks on a major city. The city also refused to pay the ransom demand—$51,000 in that case—and has faced millions of dollars in costs to rebuild and bolster defenses.

In Baltimore, Mr. Scott said he pushed city officials to strengthen cyber defenses after last year's 911 hack but that they "decided not to invest in this area."

A spokesman for Mr. Young, who became mayor May 2 upon the resignation of Catherine Pugh, said Mr. Young has directed officials to obtain cybersecurity insurance, which would help offset the cost of any future hacks.

The Wall Street Journal

By Scott Calvert and Jon Kamp

Updated May 21, 2019 4:48 p.m. ET