Bond Case Briefs

Municipal Finance Law Since 1971

To Pay or Not to Pay Hackers? Ransomware Poses a Dilemma for Governments.

Baltimore's 911 system and a range of city services in Atlanta were hijacked in the past week.

First it was Atlanta, then Baltimore.

In a matter of days, hackers launched cyberattacks in both cities, hobbling the 911 emergency response system in Baltimore and crippling a wide swath of city services in Atlanta, knocking out Wi-Fi at the nation's busiest airport and forcing city workers to keep records with pen and paper.

No evidence has emerged suggesting the attacks are connected. But in both cases the hackers used ransomware, which encrypts a victim's files and then sends a digital ransom note demanding money to decrypt them.

In Atlanta, hackers demanded $51,000 in the cryptocurrency bitcoin. City officials declined to say whether they made the payments. Baltimore officials didn't release details on the ransom amount.(One large private company, aircraft manufacturer Boeing, was also attacked on Wednesday, according to a report from Bloomberg News.)

The attacks are part of a fast-growing market in computer hacking. In a 2016, the FBI reported major uptick in ransomware attacks, with more than $200 million in payments to hackers in the first three months. That's almost 10 times the amount paid during the same period in 2015. Since the beginning of 2018, the SamSam ransomware — which was used in the recent Atlanta attack and shut down the Colorado Department of Transportation for several days last month — has raked in more than $1 million from 30 organizations.

Ransomware isn't expensive to design or purchase, and a person with even moderate coding experience can alter it to exploit leaks in a specific system's protective firewall. The odds are on the side of the hackers.

"They only have to be right once. Your anti-malware has to be right 100 times," says Tom Gilbert, chief technology officer at Blue Ridge Networks, a cybersecurity firm based in Northern Virginia.

Ransomware is a boom economy because organizations are often quick to pay.

"The economics of being a bad guy on the internet are just too good," says Oren Falkowitz, who spent seven years with the National Security Agency before co-founding Area 1 Security, a private firm.

But should they pay?

Public entities have sometimes been willing to pay the ransom demands since the hackers tend to ask for a relatively low amount of money. Madison County, Ind., for instance, paid $21,000 to regain

access to its data, and the Los Angeles Community College District forked over $28,000 to hackers.

But the San Francisco Metropolitan Transit Authority refused to pay $73,000 to the hackers who froze the agency's computer system on Thanksgiving weekend — one of the busiest travel times — in 2016. By the following Monday, the agency had regained control of its system.

The FBI advises organizations hit by ransomware not to pay. There are no guarantees the hackers will return the hijacked data. And the agency argues that paying off hackers only encourages more attacks.

"Paying a ransom not only emboldens current cybercriminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity," former FBI Cyber Division Assistant Director James Trainor said in a statement in 2016.

Government agencies are vulnerable because they're often underprepared.

"What makes the cyberattack on Atlanta so pernicious is the lack of preparation. The facts are, this is a very common phenomenon," says Falkowitz, the cybersecurity expert.

Indeed, city computers in Atlanta were infected in last year's WannaCry outbreak, which also disabled systems across the globe, including the networks of FedEx, Honda and several state-level government agencies in India.

More than 90 percent of ransomware infections come from phishing attacks, in which unwitting users are enticed to open a file or click on a link containing the malware. Falkowitz says training users to fight that impulse is a losing battle, which is why organizations need to invest in better security.

"Humans are curious, and we are talking about organizations that have hundreds of thousands of people," he says. "Someone is going to click on a link."

A virus' impact can be felt along after the initial attack. Worms like SamSam are designed to hide in the system even after a security firm flushes the computer network and patches holes in the firewall. The same worm can mutate and begin to attack other still-unprotected portions of the network.

That's precisely what happened in Colorado: SamSam infected the system in late February and then again, in a mutated form, days later.

Government agencies, says Gilbert, need to do a better job of partitioning their networks. Not every piece of data needs to be shared and not every department needs to be open to the internet.

"The absolute critical aspects of an operation really have no business being directly connected to the internet," Gilbert says.

GOVERNING.COM

BY J. BRIAN CHARLES | MARCH 29, 2018