Cyberattacks wakeup call for local governments to prepare

30 March 2018, by Kate Brumback

Atlanta police officers initially had to write reports by hand. Residents still can't pay water bills online. Municipal court dates are being reset. All are fallout from a ransomware attack last week that hobbled the city's invisible infrastructure.

Another ransomware attack hit Baltimore's 911 dispatch system over the weekend, prompting a roughly 17-hour shutdown of automated emergency dispatching. The Colorado Department of Transportation suffered two attacks just over a month ago. And the North Carolina county that's home to Charlotte totally rebuilt its system after a December attack.

For cash-strapped local governments, paying for robust protection against the invisible menace of a cyberattack can be a hard sell. But cyberattacks continue to proliferate, and experts say preparation and strong defensive measures are necessary to avoid the crippling effects.

"As elected officials, it's often quite easy for us to focus on the things that people see because, at the end of the day, our residents are our customers," Atlanta Mayor Keisha Lance Bottoms said at a news conference Monday. "But we have to really make sure that we continue to focus on the things that people can't see, and digital infrastructure is very important."

Although it's vital to make sure systems are up to date and have the latest patches, malware evolves so quickly that experts also stress the importance of comprehensive backups and a quick response when an attack does happen.

"I don't think any security is flawless," said Craig McCullough, a vice president at security firm Commvault. "I always approach it from the standpoint of it's not a matter of if but when, and when it happens, are you prepared? Are you going to be able to get your data back?"

Governments, public agencies and companies need to know what data they have and make sure it's backed up. Software and hardware can be replaced, but data is much more difficult, McCullough said.

A quick response can help minimize the damage, said Dmitri Alperovitch, chief technology officer of security firm Crowdstrike. If a threat is detected immediately after it enters the network—for example, when someone clicks on a link in a phishing email or through a vulnerable server—it might be possible to stop before it spreads beyond the initially infected computer, he said.

Atlanta officials won't say whether they'll pay the $51,000 ransom, though Bottoms has said all options are on the table. Mike Cote, president of Secureworks, a security firm hired by Atlanta, has said they know who's behind the attack but aren't releasing that information.

Cybersecurity experts say the attack is consistent with the SamSam group, which is known as a sophisticated attacker and negotiator, said Jake Williams, founder of security firm Rendition Infosec.

Unlike other ransomware that might raise alarms upon infection, SamSam compromises machines without immediately locking up their files. That access is then used to spread through the network "before they press the encrypt button," Williams said.

"They put you into an extreme pain point position where paying is actually an attractive option," Williams said

He said he regularly tells clients they must make a business decision on whether to pay. He acknowledges that can be more difficult for governments, whose rules might block them from spending public funds on extortion.

Although Atlanta's critical physical infrastructure—including the city's airport, emergency response systems and water safety and treatment—were not directly affected, other departments are operating manually and some services have been suspended. Nuisances at first, issues caused by the outages could have compounded effects if they persist.

The mayor has been cautious, declining to give a timeline for when things might be up and running again after the cyberattack announced March 22. She has repeatedly said the investigation and recovery is "a marathon, not a sprint," and her focus is on making sure the city's network is safe moving forward.

But the road could be long.

The Colorado Department of Transportation was hit by a SamSam attack on Feb. 21 and again on March 1, and it was back to 80 percent functionality by Thursday said Deborah Blyth, the state's chief information security officer. Luckily, they had strong backups so they didn't even think about paying the ransom, she said.

In the weeks since the attack, they've implemented two-factor authentication for remote access and accelerated the implementation of other security measures that were already planned.

In Mecklenberg County, North Carolina, where Charlotte is located, it took a little more than 60 days for things to return to normal after a ransomware attack that began with a phishing email in December.

County officials didn't pay the ransom after consulting with federal authorities and realizing their data was backed up so they didn't need to pay to get it back, County Manager Dena Diorio said. But the process was still tedious as they had to essentially rebuild the system.

The county has taken steps to prevent another attack, including making its email system more secure and limiting employees' internet access. And they have more expensive plans—segmenting their data and moving to a cloud-based system—that will take about two years to implement, Diorio said.

Remembering the scary early days, Diorio had advice for her counterparts in Atlanta: "All I can say is: Don't panic and stay focused."