North Carolina county's ransomware recovery will take days

December 7 2017, by Jonathan Drew

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

A North Carolina county was working Thursday on the lengthy process of fixing its computer systems after refusing to pay off a hacker who

used ransomware to freeze dozens of local government servers.

It will take days to restore Mecklenburg County's computer system, local officials said, leaving residents in North Carolina's most populous metro area facing delays or disruptions to county services. Deputies were processing jail inmates by hand and building code inspectors switched to paper records after a county employee unleashed the malicious software earlier this week by opening an email attachment.

County manager Dena Diorio said late Wednesday that the county will not pay the $23,000 demanded by the hacker believed to be in Ukraine or Iran. Diorio said it would have taken days to restore the county's computer system even if officials paid off the person controlling the ransomware, so the decision won't significantly lengthen the timeframe.

"I am confident that our backup data is secure and we have the resources to fix this situation ourselves," said Diorio. Describing county services, she said: "We are slower, but we are up and running."

The county of more than 1 million residents includes Charlotte, but the city government appears not to have been compromised by the attack. The state's largest city issued a statement that its separate computer systems have not been affected and that it severed direct connections to county computers.

The computer problems haven't affected the processing of emergency calls because they are handled by the city, said Mecklenburg County Sheriff's Office spokeswoman Anjanette Flowers Grube.

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

Such attacks are becoming more common—and more sophisticated. A security expert said he reads about a local government being targeted every couple of months. For example, a hacking attack in late 2016 on San Francisco's mass transit system led its operators to allow free rides over part of a weekend because of data problems.

Ross Rustici, senior director of intelligence services at the firm Cybereason, said local governments are "easy targets" because of their older equipment and software. Paying the ransom can often be cheaper than other ways of recovering the data.

"Once you're in that situation, you really have no good option, so a lot of people and companies end up paying," he said.

The North Carolina cyberattack has caused delays for the Mecklenburg County jail and disrupted other county services ranging from domestic violence counseling to tax collection. Sheriff Irwin Carmichael said it's taking longer to manually process arrestees, as well as inmates due to be released.

Calls to a county domestic violence hotline are rolling straight to voicemail, so counselors are checking messages every 15 minutes, officials told reporters. And the social services department is working to recreate its daily itinerary of 1,600 rides for elderly patients with medical appointments. Recurring appointments that account for most of the rides are less of a problem than those for patients who make one-time reservations.

Meanwhile, payments to the tax office must be made with a check, cash or money order, and code inspectors have been slowed down by having to use paper records, according to a list of affected services.

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

Diorio said county computers began to suffer Monday from the attack, which was publicly revealed the next day. A forensic examination shows 48 of the county's 500 servers were affected, Diorio said, adding that county government officials believe the hacker wasn't able to gain access to individuals' health, credit card or social security information.

The compromised servers have been quarantined, and even potentially healthy parts of the system were shut down to avoid spreading the malicious program, said Keith Gregg, the county's chief information

officer. But without getting the compromised servers unlocked, the county will have to rebuild significant parts of the system.

Diorio said county technology officials will use backup data from before the ransomware attack to restore the system, but the rebuild will take "patience and hard work."