Georgia county's experience shows perils of ransomware

October 21 2019, by Sudhin Thanawala

In this Sept. 12, 2019 photo, County Sheriff Janis Mangum stands in a control room at the county jail, in Jefferson, Ga. A ransomware attack in March took down the office's computer system, forcing deputies to handwrite incident reports and arrest bookings. (AP Photo/Sudhin Thanawala)

On the first Saturday in March, computer screens at the 911 dispatch

center in this small town went dark.

Staff at the county jail around the same time could no longer open cell doors remotely with electronic controls, and sheriff's deputies lost the use of their laptops to look up license plates.

Jackson County was under a ransomware attack.

"It really crippled us as far as just made it harder for our folks to work and do their jobs," Sheriff Janis Mangum said.

Ransomware attacks have taken out computer systems at law enforcement agencies and local governments around the country in recent years, forcing them to revert to pen and paper for tasks typically done in an instant on computers.

Ransomware renders files inaccessible unless a computer user pays thieves to release them.

The attacks have slowed commerce by making electronic copies of real-estate records inaccessible and taking down online payment features.

They can also endanger people when they affect critical law enforcement systems or school security.

Officials at Flagstaff Unified School District in Arizona closed schools for two days in September after ransomware forced them to disconnect from the internet, taking down security and information systems. The move disabled badge scanners that control building access and prevented administrators from retrieving computerized lists of student medications, said district spokesman Zachery Fountain.

Baltimore in 2018 and Riviera Beach, Florida, earlier this year also lost

911 dispatch functions.

In July, a ransomware attack forced the Georgia Department of Public Safety to shut down laptops that troopers use in their patrol cars to monitor emergencies and prepare traffic citations, Lt. Stephanie Stallings said. They had to write tickets by hand.

"We hadn't ordered a ticket book in a really long time because there was no need for it," Stallings said.

Law enforcement officials and cybersecurity experts said they were not aware of ransomware causing delays that led to death or serious injury.

Officials in Jackson County insisted they were able to find ways to work around the attack. But details they provided show that it made law enforcement officers more vulnerable and could have hindered emergency responses in the rural county of about 70,000 people northeast of Atlanta.

In this Sept. 12, 2019 photo, Jackson County Sheriff Janis Mangum is shown at her office, in Jefferson, Ga. A ransomware attack in March took down the office's computer system, forcing deputies to handwrite incident reports and arrest bookings. (AP Photo/Sudhin Thanawala)

On a tour of the sprawling jail on a recent morning, the sheriff pointed out a central command system that allows staff to monitor inmates and remotely open their cells. Mangum also stopped at a videoconferencing system that lets inmates talk to family from their cell blocks.

Both went down during the attack, requiring guards to go into cell blocks to open doors and escort inmates to family visits. The additional contact increases the risk to guards.

"We don't like to do a lot of inmate movement," she said.

At the 911 center next door, dispatchers lost the computers that allow them to enter calls and monitor the locations of available emergency responders.

Dispatchers, instead, took notes by hand and relied on printed maps of the county and paper logs to keep track of emergency responders in the field, said LouAnn David, the county's E-911 director.

"It's a little bit more difficult to see who you've actually sent somewhere, so that you know who's available," she said. "It's a lot to keep up with."

The cybersecurity firm SecuLore Solutions has used news accounts to document nearly 400 cyberattacks over the last two years against public safety agencies and local governments, more than a quarter of them involving ransomware. And that's likely a fraction of the actual number since smaller attacks that don't affect services probably go unnoticed, said Tim Lorello, the company's CEO.

Other big cities that have faced ransomware attacks include Atlanta and Newark, New Jersey. Hackers targeted more than 20 local governments in Texas in a coordinated attack in August that officials characterized as unprecedented in its size.

"Public agencies are particularly attractive because they are 24-7," Lorello said. "A hacker thinks it's more likely that that the agency will pay the ransom and try to get back online."

Small counties, cities and agencies may also not have the money to upgrade their systems and keep them secure, said Tyler Hudak, with the information security firm, TrustedSec.

"If I were an attacker i would try to find somebody who had valuable data and did not have potentially the resources or means to protect that data properly," he said. "City governments definitely fall into that category."

Jackson County paid $400,000 to obtain a decryption code that allowed it to restore computer systems, county manager Kevin Poe said.

Still, dispatchers were without computers for about two weeks, according to David.

"It was very traumatic, very stressful," she said. "We're not a huge agency, so I can't imagine how it would be for agencies that are so much bigger than we are. It would have to be a triple nightmare for them."