How hackers could cause chaos on America's roads and railways

April 27 2018, by Jenni Bergal, Stateline.org

Credit: CC0 Public Domain

When hackers struck the Colorado Department of Transportation in a

ransomware attack in February and again eight days later, they disrupted the agency's operations for weeks.

State officials had to shut down 2,000 computers, and transportation employees were forced to use pen and paper or their personal devices instead of their work computers. Staffers whose computers were infected didn't have access to their files or data, unless it was stored on the internet, and the attack affected the payroll system and vendor contracts.

It could have been a lot worse: The Colorado hacks didn't affect traffic signals, cameras or electronic message boards, and state information technology officials, who refused to pay the ransom, said the system had been 95 percent restored as of last week.

Transportation systems are ripe targets for cybercriminals, according to cybersecurity experts, and many state and local government officials are only now waking up to the threat and realizing they need to beef up their defenses.

"A cyberattack or threat could affect everything from municipal transportation to high speed transit rail that operates between cities," said Srini Subramanian, a state cybersecurity principal at the consulting firm Deloitte & Touche LLP. "It could create crashes or chaos on the highways or even on city streets."

The Colorado incidents have transportation officials, who normally busy themselves with more routine matters, thinking more critically about system security.

"DOTs are traditionally built around building and maintaining asphalt and concrete. That's our bread and butter," said Alan Davis, an assistant state traffic engineer for the Georgia transportation agency who serves

on a national panel researching the best ways to prepare transportation systems for cyberthreats. "But there's also this other world that operates that infrastructure. This world is a new thing for a lot of DOTs."

In February, Maryland Department of Transportation Secretary Pete Rahn told a meeting of the American Association of State Highway and Transportation Officials that security breaches are a big concern for his agency, which oversees public transit, highways, tolls, a port, an airport and the motor vehicle administration.

If hackers get into the network, he said, "they can play with our trains, traffic signals, variable message boards. We've never had to think about these things before."

Rahn's fears are not far-fetched.

It's not uncommon for hackers to take control of electronic messaging signs on roads, often as a prank. Some will display obscene language, jokes or personal messages. Usually, they access the signs remotely through a network connection in which a password may not be reset or even used at all.

But hacking into a transportation system can have more serious consequences. In 2008, a 14-year-old computer whiz used a device to hack into a tram system in Poland, derailing several trains and injuring at least a dozen people.

State and local governments face growing threats from hackers and cybercriminals, including those who use ransomware: malicious software that hijacks computer systems, encrypts data and locks machines, holding them hostage until victims pay a ransom or restore the data on their own.

In 2016, a ransomware attack struck San Francisco's light rail system, disrupting its computer system and email. Hackers requested about $73,000 in bitcoin to unlock the agency's computers, which the Municipal Transportation Agency refused to pay. As a precaution, it turned off ticket machines and fare gates in its stations, allowing customers to ride free during some of the weekend.

Last fall, Sacramento's regional transit agency was hit with a ransomware attack demanding it pay a single bitcoin, then worth about $8,000, to get control of its website back. Transit service continued, but the website took two days to restore, and city officials met with federal security officials.

Atlanta has been reeling from a ransomware attack in March that crippled several city offices and interrupted services. Residents couldn't pay bills or traffic tickets online, the municipal court couldn't view cases, police had to file paper reports, and inmates had to be booked by hand.

Many cyberattacks on state and local government have disrupted day-to-day operations or targeted the personal data of millions of residents. But cybersecurity experts and transportation officials caution that in today's digital world, where everything from traffic lights and road sensors to trains and ports are connected to computer networks—just as self-driving vehicles will be—hackers could do a lot more damage.

"There's a real emerging concern about this in state DOTs because everything is becoming more connected," said Doug Couto, a cybersecurity and transportation consultant and former chief information officer for the Michigan transportation department. "Anything on a network or on the internet becomes vulnerable to hackers.

"We need to guard against cyberattacks because they're exponentially

increasing," Couto said. "It would be fair to say that they hadn't been thinking about it a lot in DOTs."

Georgia's Davis said states' traffic operations centers, which monitor traffic signals, electronic message signs and incident response units that help disabled motorists, could be crippled by cybercriminals.

He said his agency, which has its own IT department and cybersecurity team, has bolstered its defenses against hackers. He thinks it's a good idea for state transportation agencies to have their own IT and cyber staff so they don't have to share a common network with other agencies and can be protected if the statewide system is breached.

Many transportation agencies, including Colorado's, are consolidated into statewide IT departments that handle cybersecurity, or have a hybrid setup in which IT is centralized but agencies may have a cyber analyst on staff.

And many state IT officials think it's better for one statewide department to manage the entire network, both for efficiency and to ensure that every agency is equally prepared for cyberthreats.

Regardless of where IT is located, officials say cybersecurity funding remains a serious challenge for state governments. A 2016 survey of top IT security officers from 48 states found that in most states, spending on cybersecurity was a fraction of the overall IT budget, ranging from zero to 2 percent.

Another challenge for state transportation agencies is how to protect information when working with local governments on regional transportation projects, Davis said. Sharing information on networks that aren't entirely secure can leave agencies vulnerable to hackers.

"You can build as high a wall on your side as possible, but they can go around that wall on the other side," he said. "When Atlanta had their ransomware attack, I thought, 'Uh-oh—what's our connection to the city? Do we have to pull the plug?' It turned out we were OK, but that was alarming."