Source (Bloomberg CityLab):
https://www.bloomberg.com/news/articles/2019-10-29/what-cities-can-learn-from-atlanta-s-cyberattack

What Cities Can Learn From Atlanta’s Cyberattack

Atlanta’s chief information officer explains why it’s better to spend millions recovering city computer systems from a cyberattack than to pay ransom.

Atlanta Chief Information Officer Gary Brantley speaks at CityLab 2019 in Washington, D.C.*Kristoffer Tripplaar/CityLab*

Adam Sneed
October 29, 2019, 8:33 AM CDT

In March 2018, hackers targeted Atlanta’s computer networks. Demanding $51,000 in bitcoins, the cyberattack held the city hostage for nearly a week. Some city services reverted to pen and paper to continue operations.

But the city refused to pay: It didn’t want to reward and encourage more ransomware attacks, and there was no guarantee that systems would be restored even if it paid. Ultimately, the financial hit to the city was far higher than the ransom. One city report uncovered by the Atlanta Journal-Constitution estimated that the costs associated with the attack could reach as high as $17 million.

The episode marked an important moment of truth for the city. Atlanta was unprepared for such a major disruption, but it was clear that hackers had targeted cities before and would continue to do so for the foreseeable future. So, the city's response wasn't just about recovering from a single incident: It was also about building a foundation for responding to future attacks.

"We're not here to necessarily stop the attacks," Atlanta Chief Information Officer Gary Brantley said on a panel Monday at CityLab D.C. "We're here to prepare for the inevitable."
Atlanta is hardly alone in having fallen victim already. Newark, New Jersey, paid $30,000 to recover its systems after a ransomware attack last year. (The U.S. Justice Department says a pair of Iranian hackers was behind both the Newark and Atlanta attacks.) In Baltimore, Maryland, the city's computer systems were down for weeks this spring after the city refused to pay an $80,000 ransom. The tab for this attack could run upwards of $18 million, according to USA Today. And many other cities large and small have been locked out of their systems and forced to make the same tough choice: Pay out tens of thousands of dollars at once to (hopefully) fix an urgent problem, or spend several million more to (potentially) be in a better position for the future?

Getting governments up to speed on cybersecurity will be costly but necessary: "Bad actors are a lot more organized than cities."

Brantley, who joined the City of Atlanta about six months after the attack, says cities should commit to taking the second path.

"It's less about the attack for me, and more about your ability to respond when it happens," he said.

Since becoming Atlanta's CIO in October 2018, he has focused on building a continuity plan so city officials know how to continue operating city services even if a cyberattack takes down their networks. He compared preparation efforts to school safety drills: "When there's a disaster situation, those kids know exactly what to do," he said, because they've practiced it before.

Wendi Whitmore, IBM's vice president of X-Force Threat Intelligence, said on Monday's panel that running through such drills can reveal critical weaknesses that allow cyberattacks to take place, as well as simple prevention efforts that can protect against extensive damage. When an attack happens, city employees might find they don't know how to reach their colleagues without city-issued devices and email accounts, for example. Or an agency might know to keep backups of its data, she said, but if the backups are connected to a compromised network, they could be corrupted along with everything else.

And then there's the communication aspect. That can be especially tricky, because it can be difficult to determine the full scale of a cyberattack. Also, the public might not understand much of the technical language involved. Whitmore said she cautions clients not to offer up more information than they're certain of. Atlanta, for example, originally said people who had made financial transactions with the city should monitor their bank accounts—conveying a threat that wasn't really present, Whitmore said, and inciting more fear than was necessary.

Ultimately, Whitmore and Brantley agreed, getting city governments up to speed on cybersecurity will be costly but necessary. "Bad actors are a lot more organized than cities," Brantley said.

"Breaches are going to occur," Whitmore said. "But if you can limit the impact, you have a win."