2-The New Yorker-Atlanta

Save Story

Save this story for later.

Last Thursday morning, the Atlanta city councilmember Howard Shook walked into his office and immediately began following the urgent recommendation of his I.T. department: “Principally,” he recalled, “turn off everything.” Shook, who represents District Seven, in Atlanta’s northeastern metropolitan area, has three computers in his office, all of which had been infected with ransomware. “Sixteen years’ worth of information—gone,” he told me. “Every e-mail. All our contacts. All our files: city policy, district-specific projects, activities. It’s devastating.” A few days later, his office was given a clean, unused laptop from the city-council inventory. The I.T. department has since provided new passwords and strengthened the e-mail filters *[Rebuild]*“to the point where there’s a lot of stuff that’s probably not getting in that should get in.”

Shook currently serves as chair of the city’s finance committee; in years past he has been the city council’s president pro tempore and has served on each of its seven committees. “There have been plenty of internal debacles that I’ve had to deal with over the last two decades,”

he said. “But this is by far the biggest external debacle. We’ve been assaulted by a cybercriminal on a massive scale.” The Times called last week’s hack into the computer network of the largest city in the southeastern United States, which is home to the Centers for Disease Control and Prevention and the Coca-Cola Company, “one of the most sustained and consequential cyberattacks ever mounted against a major American city *[Disappointment]*.”

It wasn’t immediately obvious to Shook, who describes himself as “not a tech person,” what exactly being hacked mean *[Disappointment]*t.

SamSam, a “shadowy hacking crew,” as the Times described it, had reportedly penetrated the city’s computer network with ransomware —a

decade-old technology that infects a computer or a network and blocks access to personal data through encryption—and was holding access to the network for ransom: approximately fifty-one thousand dollars, to be paid in bitcoin. Atlanta was the latest in a series of ransomware victims: FedEx, Britain’s public-health system, Boeing ,

and many other public and private-sector entities have been targeted similarly in recent years . But Atlanta is the largest American city to have fallen victim to the ploy. (Baltimore suffered a “limited” ransomware breach this past weekend, according to city officials, that affected its 911-dispatch system for twenty-four hours. And five computers in Atlanta’s network were reportedly breached last year .) The Atlanta hack has, among its many consequences, interrupted wireless Internet at the busiest airport in the country; made courts unable to validate warrants; created parking-system problems ; and, perhaps most consequentially, initiated the loss—maybe permanent—of digital city files. *[Disappointment]*

A week after the hack started, Atlanta’s recently elected mayor, Keisha Lance Bottoms, still has not confirmed whether the ransom has been paid in this “hostage situation,” as she has called it. “ Everything is up for discussion ,” she told reporters. (Bottoms has been busy with damage control, tweeting to her constituents about the job-threatening inconvenience of not being able to pay their parking tickets online, and the security of their personal-financial information .

The city’s official F.A.Q. Web page about the hack went online this morning.) A few sources, who asked to remain anonymous, have told me that the ransom, though a relatively—even strangely—modest sum for a city with a budget in the billions, has likely not been remitted. Shook said that “the city does not appear to have a policy regarding the paying of ransoms.” One city official told me, “We’re so fucked. We’re not paying the ransom. There’s no point. We’ll bite the bullet and rebuild our system in a stronger way.” *[Rebuild]* Another frustrated employee, who has worked for the city for more than a decade, said the city never spends enough to

sufficiently address these sorts of problems. “They’re all about lowest bidder,” he said. *[Disappointment]*

In the meantime, Shook and others are perplexed by the seemingly random focus of the attack. The District Eight council office, next door to Shook’s, also has three computers; two of them are still functional.

“It’s the same on down the hall,” he said. In any case, he doesn’t see much good in paying a ransom. “The damage is done,” he said. “Stuff is lost. I’m a tiny little example, but my computers—the contents have to be euthanized.” He added, “We’ll rebuild the contacts, but, for me, the lesson learned is: this longtime goal of moving to a paperless society looks a lot less exalted now than it did a week ago. I’d give anything for a hard copy of everything I lost.”

A federal criminal investigation is currently under way. So far, federal officials have not revealed any details about how the attack occurred, which individuals carried it out, or why. (The SamSam crew was identified by researchers at an Atlanta-based security firm that is assisting the city in its response.) Shook met with the federal cybersecurity team—“Secret Service, Homeland, F.B.I., everyone but Jack Bauer,” he said—and has busied himself learning about hacking crimes generally. “This happens to individuals. This happens to private companies. To public entities. Welcome to the evils of the twenty-first century. I can’t wait to find out how this pathogen entered the city system.” A former city employee, who left her job last year, told me, “When I was there, I was appalled at how shaky the I.T. infrastructure was. Every time there was a network outage the I.T. department sends a notification. I got those notifications so frequently that I just started deleting them.” *[Disappointment]*

The city’s executive committee had a closed-door session yesterday to discuss the attack. The city’s administration told them that, moving forward, there would be more sophisticated strategies in place to thwart hackers. Computers would be rebuilt and workers retrained with anti-malware services. *[Rebuild]* “What I don’t want to do is spend a whole bunch of money and then have this happen again,” Shook said. “But I don’t know what the model for a solution is, unless it’s military-grade, nuclear-

submarine-type stuff.” He went on, “There’s a lot of really smart criminals out there. We have ninety-seven hundred city employees.

All it takes is for one of them to open an attachment they shouldn’t open. Well, that’s hard to defend.”

Charles Bethea is a staff writer at The New Yorker.

More: Atlanta Cyberattacks Cybersecurity Hacking

The Daily

The best of The New Yorker, every day, in your in-box, plus occasional alerts when we publish major stories.

E-mail address

By signing up, you agree to our User Agreement and Privacy Policy & Cookie Statement .

Read More