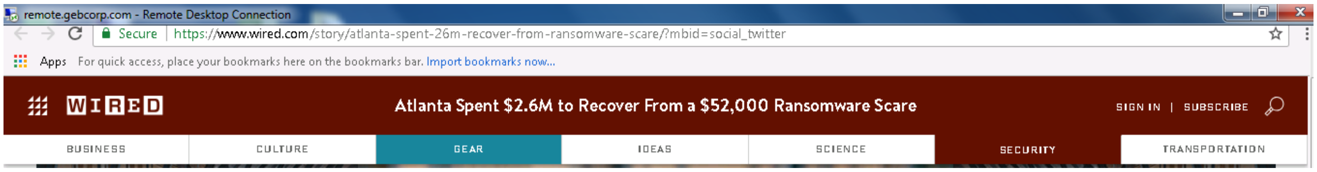
remote.gebcorp.com - Remote Desktop Connection

Secure | https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/?mbid=social_twitter

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

WIRED Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare

ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE

LILY HAY NEWMAN

APRIL 23, 2018

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare

Whether to pay ransomware is a complicated—and costly—calculation.

Whether to pay ransomware is a complicated—and costly—calculation.

The City of Atlanta spent more than $2.6 million on emergency efforts to respond to a ransomware attack that destabilized municipal operations last month. Attackers, who infected the city's systems with the pernicious SamSam malware, asked for a ransom of roughly $50,000 worth of bitcoin. (The exact value has fluctuated due to bitcoin's volatility.) Atlanta officials haven't said whether they paid the ransom, or even tried, but it seems that they may not have even had the chance; the attackers quickly took the payment portal offline, and left the city to fend for itself. So far, the recovery has been far more costly than the initial demand.

The Atlanta Department of Procurement lists eight emergency contracts initiated between Match 22 and April 2 with a total value of $2,667,328. The bulk of the expenditures relate to incident response and digital forensics, extra staffing, and Microsoft Cloud infrastructure expertise, presumably all related to clawing back the systems that the hackers had frozen. The city also spent $50,000 on crisis communications services from the firm Edelman, and $600,000 on incident response consulting from Ernst & Young.

'It can be very expensive, and defense is not an easy thing.'

While the security and law enforcement communities generally discourage victims from paying ransoms—it'll only encourage them, the logic goes—it's sometimes not so clear cut. It complicates matters further that attackers intentionally set their ransom prices at a level they think victims can afford. They want to maximize how much they walk away with, while still offering a "bargain" to targets versus doing the work to rebuild systems and restore from backups. The US government "does not encourage paying a ransom to criminal actors," the FBI notes in a "Ransomware Prevention and Response" document. "However, after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting system from backup."

Every situation, in other words, has its own financial and ethical calculus. In Atlanta's case, refusing to pay and investing in remediation will likely improve Atlanta's cyberdefenses for the long term. But paying the premium to do these improvements during a crisis burned through taxpayer dollars that could have been spent elsewhere. And while the bill seems high, it's actually not entirely out of line for remediation on this scale.

"What Atlanta paid is maybe not a bargain, but I think they probably did pretty well," says Chris Duvall, senior director of The Chertoff Group, which specializes in risk management. "We had a private sector client, a relatively small company that was about $60 million in revenue, they ended up paying about $3.1 million after a ransomware attack, because they had all the incident response, plus insurance claims, privacy monitoring, and contractual hits for missed services. It can be very expensive, and defense is not an easy thing."

Though a municipality doesn't have the specific obligations of a private company, it still has plenty of crucial considerations and costs. Atlanta's ransomware attack impacted five of the city's 13 local government departments, and disrupted many functions people rely on every day, including the Police Department records system, infrastructure maintenance requests, and the judicial system. The attack also hindered revenue collection; residents weren't able to pay their water bills for days. The City did not return a request from WIRED for comment.

'Emergency support and overtime costs phenomenally more than just handling the issues.'

Paying the ransom up front might have saved the City of Atlanta time and money—and on paper would have cost several orders of magnitude less than the eventual cure—but it's not quite as simple a call as it seems. City officials had no guarantee that attackers would actually release their systems upon payment. Or even if the hackers did decrypt the infected devices, the city's digital infrastructure could still been weakened by the attack. There is also evidence that Atlanta was behind on addressing known vulnerabilities in its networks, so seizing the ransomware attack as an opportunity to invest in proper defense may offer more assurance that things have improved than simply paying a ransom and continuing to put off substantive upgrades.

"Emergency support and overtime costs phenomenally more than just handling the issues," says Jake Williams, founder of cybersecurity firm Rendition Infosec. "In other words, upgrades that might have cost $100k in normal budgeting might cost $300k-plus in emergency spending during an incident."

Though it's tempting to say that it's worthwhile to take the easy savings by paying ransoms, experts are reluctant to ever recommend it. Instead, they emphasize that investing in software updates, backups, and network segmentation now can genuinely pay off for institutions later if they are targeted by ransomware.

"It may be a Pollyanna belief, but you’re only feeding the problem if you pay," says Dave Chronister, founder of the corporate and government defense firm Parameter Security. "It only works if people are actually paying it, and instead that money could go a long way to actually fixing your stuff beforehand."

Which doesn't help Atlanta much. But it may help the next city that the SamSam attackers strike.

This preceding article may be found online at: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

ACCG SUITE
TECHNOLOGY SOLUTIONS FOR LOCAL GOVERNMENT

Over the last year, several Georgia counties have been hit with Ransomware. Through ACCG SuITe, the association can assess your systems and help you to put protections in place to avoid this situation in your county.

For more information, contact Brent Williams at 404.522.5022 or bwilliams@accg.org.