Local Governments Held for Ransom: Lessons Learned from the Atlanta Cyber Attack

Rhonda Collins, Asst. City Attorney, City of Atlanta
Roy Hadley, Special Counsel, Adams and Reese LLP

I. Introduction

"On Thursday, March 22, the City of Atlanta experienced a ransomware cyberattack that affected multiple applications and client devices. As a result, some City data is encrypted and customers are not able to access City applications. Atlanta Information Management (AIM), the City's technology department, is working to restore service."[1] These three sentences concisely summarize the cyberattack that was perpetrated against the City and the high-level impact of the attack. However, these two sentences, and likely no two sentences, can explain the initial shock and confusion that employees felt when they tried to access their work files and the City's most critical systems.

The morning of the attack, many employees continued unsuccessful attempts to access encrypted files by rebooting machines and repeatedly calling the help desk. As the day unfolded and the City learned more details about the attack, it became clear to everyone that criminals had not only attacked the City's systems, but that they had also demanded a ransom payment of $51,000 in Bitcoin.

Unfortunately, the City of Atlanta's cyberattack is not unique. Instead, instances of digital extortion are becoming a common occurrence across all organizations. In fact, the World Economic Forum's Global Risk Report 2018 identified cyberattacks and data fraud or theft in the top five (three and four, respectively) global risks by perceived likelihood of these events

[1] The City of Atlanta's website, https://www.atlantaga.gov/government/ransomware-cyberattack-information (The City of Atlanta created a ransomware attack information hub, which contains frequently asked questions and answers).

occurring.[2] News reports are rife with examples of high-profile attacks being perpetrated against many of the most recognized global brands. Companies such as Equifax, Home Depot, Sony Pictures, and FedEx, have experienced massive attacks and data breaches. More recently, cyberattacks on hospitals and governmental entities are garnering attention because these attacks potentially threaten the critical services that individuals rely upon each day. Attacks have recently occurred in Savannah and Hinesville, GA, Allentown, PA, Dallas, TX, and Baltimore, MD. The attack in Baltimore, MD affected its 911 dispatch system, which further underscores how these attacks threaten individuals' safety.[3]

Cyber threats are becoming more hostile and frequent, so all organizations must understand how to best protect themselves against these attacks and what to do when they occur.

This paper explores some of the events that occurred after the initial attack and how the City of Atlanta moved forward to remediate and recover from the attack. The actions taken by the City of Atlanta include many of the actions that any organization facing this type of attack would take. However, all organizations are different, and each organization should have its own plan for protecting against and responding to cyberattacks. With that being said, the purpose of this paper is to illustrate one example of how a ransomware attack impacted a city's operations. In addition, this paper will educate you about the issues surrounding cyberattacks to give you practical guidance about how attacks happen, how you work to prevent them from happening, and how to respond if they occur.

II. What is Ransomware?

[2] World Economic Forum, *The Global Risks Report 2018, 13th Edition* (January 17, 2018), available at http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

[3] Sarah Meehan and Kevin Rector, *In Wake of Baltimore 911 Cyberattack, Officials Urge Layered Protections*, The Baltimore Sun, March 30, 2018, available at http://www.govtech.com/security/In-Wake-of-Baltimore-911-Cyberattack-Officials-Urge-Layered-Protections.html.

Ransomware is a type of malicious software or malware that locks your system and encrypts files. In exchange for payment, the hacker promises to release the hostage files. Hackers usually demand Bitcoin or another cryptocurrency for payment. These currencies are demanded because they provide anonymity to the hackers.

Hackers perpetrate these attacks in numerous ways. One common method of attack is a phishing scam via email. Phishing scams use social engineering to trick a user into clicking a link that opens an attachment because the emails are designed to look trustworthy. After a user opens an infected attachment, it takes over and encrypts the user's computer. Other types of malware exploit vulnerabilities in systems, such as web servers, to execute attacks. Attacks against personal computers can encrypt the entire system or just specific files. Ransomware can also delete or permanently corrupt files so that the files are destroyed forever.

III. Attack Against the City of Atlanta

Around 5:40 am on March 22, 2018, information officials at the City of Atlanta realized that something was amiss with the City's network. Later that morning as employees powered up and logged into their computers it became obvious that the unusual activity was a full-scale ransomware attack. Some employees were greeted with messages on their screens demanding Bitcoin payments, and other employees just saw manipulated icons and new extensions appended to their files. Just like with any other crime, the first few hours of the attack were crucial for mitigating the damage and determining the next steps forward.

There are many actions that the City of Atlanta undertook to respond and recover from the cyberattack. The select points below provide a general overview of the essential actions the City of Atlanta took to respond to and recover from the attack.

A. Communication

Cyberattacks are crimes, so upon discovering the attack, the City immediately contacted law enforcement. Law enforcement must be notified immediately to assess the incident and to begin an investigation. After contacting law enforcement, the City contacted other key partners, including its insurance carrier, outside counsel, government partners, and the media. Most importantly, the City, in partnership with law enforcement and its key partners, developed a strategy to communicate the details of the attack to City employees and the public. In communicating with the public, the City balanced the sensitivity of the ongoing investigation with informing its nearly 8,000 employees and its residents about the status of the attack.

At the beginning phases of the incident, the City shared as much as possible to keep the City operating without compromising the investigation. Pending further investigation, City officials did not know whether individuals' data had been compromised, but the state of Georgia, like many other jurisdictions, requires organizations to notify affected individuals in the event of a data breach. Under Georgia law, a data collector[4] must report a breach of the security of a system[5] in the "most expedient time possible and without unreasonable delay."[6] This notification requirement is triggered in the event that an individual's unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[7] In an abundance of caution, the City notified all employees and residents of the breach and instructed everyone to

[4] "Data collector" means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information. O.C.G.A. §10-1-911 (2).
[5] "Breach of the security of the system" means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. O.C.G.A. §10-1-911 (1).
[6] O.C.G.A. §10-1-912 (a).
[7] *Id*.

monitor their personal accounts via the City's website, social media accounts, and news outlets. As the City learned more facts about the attack, the City continuously updated all potentially impacted individuals about the incident and maintained a running list of "frequently asked questions" on the City's website to ensure that all individuals had access to complete information.

B. Collaboration

Early in the response efforts, the City identified the key individuals who would need to be involved in the response. As many of the City's critical systems were impacted, the City quickly realized that its Office of Emergency Preparedness would be the best single point of contact for the response efforts. That office, along with the Departments of Information Management, Law, and Procurement coordinated many of the very first conversations with law enforcement, outside counsel, the City's insurance provider, and the emergency vendors. Over time, the key contacts and stakeholders shifted to address the ongoing response. For example, the roles of the City Council and the Risk Managers in the Department of Finance expanded as the initial threat was mitigated.

C. Initial Assessment and Investigation

The City acted quickly to determine what systems, functions, and operations were impacted. That task might sound simple, but during an emergency, listing every impacted City system was exponentially more difficult to accomplish, especially without the assistance of technology. Early on, the City hired a security firm to assist with the City's response. Additionally, the City also enlisted the assistance of management consultants to document the state of operations. The baseline assessments that these firms conducted illuminated all of the City's actions going forward. Specifically, the City was able to identify the critical enterprise applications that were

impacted because of the forensics that the security firm performed and because of the accounts provided from frontline employees about how their day-to-day operations were impacted.

D. Insurance

Every business and governmental entity has different network security and privacy risks, which means that cyber insurance policies can vary greatly. Ransomware attacks generally fall under a cyber insurance policy's "cyber extortion" coverage. That said, some types of claims may not be covered so it is best to work with a knowledgeable broker when obtaining coverage.

Some cyber insurance policies offer both "first-party" and "third-party" coverage, while many policies offer "third-party" coverages only. We note that if you only have "third-party" coverage only, you may find that you are uninsured in the event of a ransomware attack.

When submitting a ransomware attack claim under a cyber insurance policy, there are usually strict requirements that the cyber insurance policyholder must follow, and one misstep can leave you uninsured. As such, obtaining expert advice and counsel is generally a good idea.

With respect to ransomware, you generally will need an endorsement to cover the payment of any requested ransom. Again, however, a knowledgeable broker can help you tailor cyber coverage to your needs, including any necessary endorsements to your cyber policy.

Given that ransomware attacks are increasing – like cybercrime in general – obtaining adequate insurance is becoming a necessity.

IV. Ongoing Security Practices

1. Be proactive.
2. Educate.
3. Back up (offline and offsite backups).
4. Security patching.
5. Hire and empower a Chief Information Security Officer.
7. Continuous protection, but nothing is full proof.

9. Strong passwords.
10. Get cyber insurance.
11. Segmentation of network and network operations.
12. Communicate- But Not Too Much!!
13. Ransomware awareness plan – Emergency response planning.
14. Prioritize funding.
15. Data audit/ Risk Analysis / Maturity Assessment.
16. Check employee references/ issue particular levels of clearance and/or access.
17. Be prepared for open records and FOIA requests.
18. During/after an attack – DOCUMENT/ PLAN / BE NIMBLE, BUT SET UP CLEAR PROCESSES/ HAVE AN INCIDENT RESPONSE PLAN JUST LIKE ANY OTHER EMERGENCY.

V. Conclusion

Regardless of the protective measures that your organizations employ, nothing is guaranteed. If you or your organization is a victim, be sure to notify the appropriate parties immediately. Above all, however, having a plan, including practicing your plan, will be key to your success in the event of an attack. The account provided here can serve as a useful, practical guide for organizations seeking a basic understanding of how to prevent and respond to a cyberattack.