Cyberattacks on Courts and Other Government Institutions

By Judge Herbert B. Dixon Jr.

Like many of you who may be willing to admit it, I have laughed at my dependency on electricity many times during electrical power outages after walking into a dark room and instinctively flipping on the light switch. I realize now that our dependency on online interconnectivity and electronically stored information is even greater. Just think of the frequency you have clicked a link to access a website or performed a search for a digital file, or performed an Internet search for the definition of an unfamiliar word, or sought to learn the author of a profound quote or the name of an actor in an old movie. I am writing this column about cyberattacks because of the extreme disruption they can have on our daily lives—brought about by our new dependence on stored electronic information and access to the Internet. I'll start with a recent attack in Atlanta when city employees were instructed upon their arrival at work to not turn on their computers.

Atlanta's Cyberattack Experience

As described by the mayor of Atlanta, the city was in a hostage situation. The city's computer systems were the victims of a ransomware attack. The intruders disabled online access, encrypted files, and demanded a Bitcoin payment in return for the encryption key to regain access to the system files and other data. I cannot think of a more appropriate name to call these intruders than terrorists.

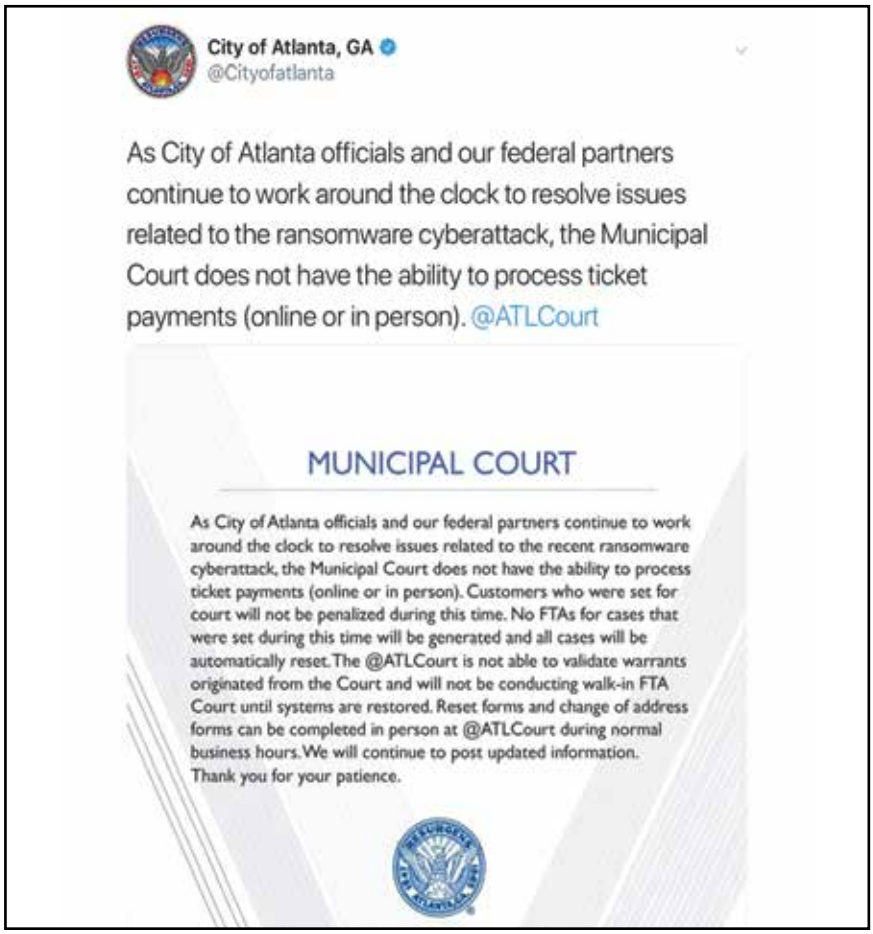
After the terrorists disabled Atlanta's computers and online presence, no one could pay traffic tickets or make online water and sewer bill payments. The Atlanta Municipal Court did not have access to its electronically stored scheduling information and could not validate outstanding warrants. Police officers had to file paper reports. Persons due in court during this interval did not receive failure-to-appear notices nor were warrants for their arrest issued. Their cases were rescheduled. The city waived late fees for those who were prevented from making timely payments to the city. I cannot imagine what it must have been like for a judge with a significant trial set that day, unable to gain access to electronically stored pleadings and pretrial rulings in the case, and having a courtroom full of impatient litigants, lawyers, and witnesses.

Atlanta's Hartsfield-Jackson International Airport, the world's busiest airport, shut down its free passenger Wi-Fi system as a precaution because of the Atlanta hacking and disabled online access to information about security wait times and flight information updates. Nearly 1,000 Atlanta employees working at the airport had limited or were locked out of access to email and the Internet.

It took about a week for employees to start receiving notices that it was safe to turn on their computers. Some systems and data were fully recovered, but not all. One member of the city council lost 16 years of data.[1] Moreover, this was not the first such attack. A Georgia-based cybersecurity firm reported that five Atlanta systems, including a webmail server, were infected nearly a year earlier in April 2017.

Atlanta is not alone in its cybervictim status. Courts and government agencies increasingly are the targets of cyberattacks. Other incidents against these institutions

Judge Herbert B. Dixon Jr. has retired from the Superior Court of the District of Columbia after 30 years of service. He is chair of the ABA Standing Committee on the American Judicial System and a member of the Techshow Planning Board. He is a former member of the ABA Board of Governors and a former chair of the National Conference of State Trial Judges. He can be reached at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.



A Twitter post by the City of Atlanta about the Municipal Court of Atlanta and their system outage following the ransomware attack in March 2018.

paint a similar picture. A few additional examples are below.

The Leeds, Alabama, Experience

In February 2018, the City of Leeds, Alabama, experienced a ransomware cyberattack in which the intruders took control of the city's computer system. As in the Atlanta event, this cyberterrorist also requested a Bitcoin ransomware payment, which at the time amounted to $12,000—about a dollar for each city resident. After paying the ransom, the city regained control of its system. In this instance, the ransom was probably less than the anticipated costs of projected downtime and expenses to recover from the attack. The reader should note that payment of a ransomware demand is no guarantee of data and access recovery after the ransom demand is paid. According to Kaspersky Security Bulletin 2016, only one of every five small to medium-size businesses that paid the ransom demand got their data back. Ouch! That adds insult to injury.

Colorado's DOT Hack

Also in 2018, just before the Atlanta attack, the Colorado Department of Transportation suffered at least two cyberattacks within a matter of weeks. The attack resulted in encrypted files, renamed "i'm sorry." Employees were directed to turn off CDOT's approximately 2,000 computers. Here, also, the cyberterrorist requested a ransom in the form of the digital currency Bitcoin. The attack caused CDOT employees to stop using their computers and use pen and paper to record their data. Following the first cyberattack, after about 20 percent of the affected computers had been restored, the second attack hit.

Additionally, because of the paralyzed computer system, the CDOT had to figure out a way to make its payroll. Employees had to use their personal devices for email and shared documents through Google. It took about three weeks after the second attack to restore 80 percent of the CDOT system.

Minnesota Judicial Branch Website Hack

After suffering two attacks in December 2015, the Minnesota Judicial Branch's website suffered a more crippling cyberattack in June 2016. This cyberattack disrupted Minnesota's website functionality for 10 days. This was not a ransomware attack. The intruders did not demand compensation in cash or Bitcoin. This cybersecurity breach was a distributed denial-of-service (DDOS) attack, the purpose of which is to deny access to the website by legitimate users. In other words, the DDOS attack overwhelmed the Minnesota Judicial Branch's website with network traffic that blocked out typical users.

Dallas Weather Alarm System Malfunction

Dallas, Texas, has a weather alarm system designed to provide a loud audible warning to the area's million residents. Just before midnight on a Friday in April 2018, all of the 156 sirens started to blare a penetrating noise, which repeated in on-and-off cycles for the next 90 minutes. The noise put the area residents in a state of confusion and caused them to look for the apocalyptic weather that had caused these warnings. The alarms blasted in 90-second intervals about 15 times during those early morning hours.

After an hour of the sirens howling, city officials provided notice to area residents that there was a system "malfunction." Officials thought the event was an inside job caused by someone who had physical access to the system. Later, city officials released word at a press conference that the system had been hacked by someone who had remote access to the system.

After determining there was no emergency, city workers turned off the sirens. Unfortunately, every time the workers turned off the sirens, they started to blare

again. Eventually, the workers shut down the entire system. Of course, the city's 911 system was overwhelmed by 4,400 calls from residents about the constant blaring of the sirens. At some point, the answer time for the incoming 911 calls reached six minutes instead of the normal 10-second interval. On social media, some residents were speculating that World War III had started. The length of time it took city officials to announce a "malfunction" as the cause of the blaring sirens led to conspiracy theories and other speculation on social media that the "malfunction" was the result of a prank, or a test run by the city to see how people panic and emergency services would respond, or a disgruntled employee, or, as television or a movie would portray such an incident, a cover-up for a well-planned art or jewelry heist or nighttime bank robbery.

Baltimore 911 Temporary Outage

Shortly after the Atlanta ransomware event, Baltimore's 911/311 computer system suffered a ransomware attack. This event was less devastating than the Atlanta disruption. Baltimore temporarily switched its 911/311 computer system into manual mode and was able to fully restore the system within 17 hours. Baltimore was either lucky or well prepared.

Conclusion

As demonstrated by these examples, hacking incidents may be motivated by several reasons: (1) greed, namely, the desire to receive a ransom payment for returning control and possession of the digital property to the rightful owner; (2) disruption of the hacking victim's normal business activities; (3) theft of private and sensitive information; or (4) a combination of these motivations. Court systems and other government institutions often possess sensitive information of individuals and organizations, making those government institutions rich targets for cyberattacks and posing the possibility of devastating losses of privacy and valuable information for individuals and entities. Whatever the reason for any hacking incident, courts and other government institutions have a responsibility to protect the information and data they hold.

The purpose of this column is not to educate courts and government agencies how to prepare for and respond to a cyberattack. If you want to know more about that subject, the Joint Technology Committee issued a report aptly entitled "Responding to a Cyberattack."[2] Nevertheless, even if you have a well-executed "Plan A" response to a hacking incident, and your "Plan A" fails, consider having plans named after the remaining 25 letters of the alphabet. In 2017, over 7.8 billion records were hacked from the numerous cyberattacks that occurred during the year. That computes to slightly more than one record per person in the world considering that the estimated world population at the end of 2017 was 7.6 billion people.

Epilogue: Thoughts for the Future

Finally, hacking efforts directed at court systems are not new. In January 2014, cyberterrorists embarked upon a cyberattack on the federal court system that resulted in a brief outage affecting websites and the Public Access to Court Electronic Records (PACER) system. For several hours, the attacks disrupted bankruptcy courts, district courts, and circuit appellate courts across the nation, though the U.S. Supreme Court's site remained up. The outages essentially shut down the ability for the court and attorneys to electronically file pleadings and orders in the PACER system for nearly four hours, ending at about 7:00 p.m. One writer summed up the situation this way

> [C]ourt officials everywhere are beginning to acknowledge the event of a cyberattack on the courts is not "if" but "when." Personal data of court patrons is at risk—compromising their identities and inviting fraud. Intrusion into the court systems could sabotage the workings of the judiciary—even introduce subversive information that could throw the outcome of a case.[3]

I hope this hint to the wise is sufficient. ■

Endnotes

1. Laila Kearney, *With Paper and Phones, Atlanta Struggles to Recover from Cyber Attack*, Reuters (Mar. 31, 2018), https://reut.rs/2EacoFH.

2. The Joint Technology Committee (JTC) was established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM), and the National Center for State Courts (NCSC). *Joint Tech. Comm., JTC Resource Bulletin: Responding to a Cyberattack* (Feb. 17, 2016), available at https://bit.ly/2xGCkLh.

3. Donna Rogers, *Gone Phishing*, Court Today (Sept. 7, 2017), https://bit.ly/213YVZ6.