Cyberattacks on Government Agencies

There were 105 known ransomware incidents involving state or municipal governments or agencies in 2022, of these at least 27 also resulted in a data breach!

City of Baltimore

Threat actors successfully deployed RobbinHood ransomware against the City of Baltimore in 2019, which ended up costing the city $18.2 million. The attack compromised the city's networks, took its email system offline, and adversely impacted its dispatch system.

- Cyber attack type: RobbinHood ransomware
- Location: Baltimore
- Cost: $18.2 million
- People affected: Undisclosed

The attackers demanded a payment of $76,000, which officials declined to pay thanks to advice from the Secret Service and the FBI, plus the city's leadership did not want to reward criminal behavior. Ultimately, however, Baltimore experienced a loss that far exceeded the ransom request.

City of Atlanta

In March of 2018, a cyber attack against the City of Atlanta crippled government services. It took nearly a third of the city's software programs offline and infected 3,789 computers. The attack impacted critical police services and the city's court system, including the loss of police dash-cam recordings related to active prosecutions.

- Cyber attack type: SamSam ransomware
- Location: Atlanta
- Cost: $17 million
- People affected: Undisclosed

The attackers demanded a ransom of $51,000 to release the government's data, payable in bitcoins, which the city declined to pay. A confidential report estimates a $17 million cost to taxpayers.
On December 5, 2018, the Department of Justice indicted Iranian nationals for their role in the attack.

City of Riviera Beach, Florida

An attack in May 2019, which began when an employee in the police department opened an infected email, took the City of Riviera's main computer system offline, affecting every department. The city's finance department was forced to manually issue payroll checks that would otherwise have been automatically deposited in employee accounts electronically.

- Cyber attack type: Phishing
- Location: Florida
- Cost: $600,000 ransom paid by insurance company; $941,000 for computer equipment
- People affected: Not disclosed

To secure the safe return of stolen data taken during the ransomware attack, city council members approved the payment of a $600,000 ransom, payable in bitcoins by the city's insurance company. Additionally, the city agreed to spend almost $1 million to upgrade computer equipment, including the purchase of 310 new desktops and 90 laptop computers.

The city's IT department also engaged consultants to add safeguards and redundancies to prevent future attacks.

Pottawatomie County, Kansas

To regain control of servers encrypted in an attack on September 17, 2021, Pottawatomie County officials agreed to pay a ransom of $71,606.25, which could be seen as a bargain considering the initial asking price attackers demanded—a cool $1 million to release control of the county's data. The attack impacted the county's driver's license system and the tax department. It persisted for two weeks.

- Cyber attack type: Ransomware
- Location: Kansas
- Cost: $71,606.25
- People affected: 150 desktop and laptop computers

In the aftermath of the attack, the IT team deployed additional sensors on the county's servers and continued their investigation to determine how the attackers breached their defenses.

Metropolitan Police Department, Washington, D.C.

An attack involving Babuk ransomware resulted in the theft of 250 gigabytes of police data, including police officer personnel files, arrest records, and intelligence memos. Screenshots shared by cybercriminals online included extensive personal data stolen from the department, as well as performance reviews and polygraph records.

- Cyber attack type: Babuk ransomware
- Location: Washington D.C.
- Cost: Not disclosed
- People affected: 22+ employees

When attackers were denied a ransomware payment of $4 million, 22 personnel files were published online, each more than 100 pages. Then, when the police department allegedly offered to pay $100,000 to prevent the release of additional data, the attackers rejected their offer.

Bernalillo County, New Mexico

In the aftermath of a ransomware attack in New Mexico, prisoners incarcerated in Bernalillo County found themselves confined to their cells. The ransomware attack had taken cameras at a local jail offline and deactivated the jail's automated doors, forcing officers to use manual keys to confine the prisoners.

- Cyber attack type: Ransomware
- Location: New Mexico
- Cost: Not disclosed
- People affected: Not disclosed

In separate attacks following the attack against the county's prison system, Albuquerque's public school system was forced to close for two days, while computer systems of Bernalillo County went offline, resulting in the inability of residents to file for mortgage loans.