

# Municipalities Held

# HOSTAGE

## Addressing the Rise of Ransomware

By Taylor Gast

2019 was a banner year for cybercriminals targeting municipalities. In particular, the frequency and scale of publicly reported “ransomware” incidents targeting municipalities rose exponentially. In May, a ransomware incident effected Baltimore, and while the hacker demanded roughly \$75,000, the incident cost the city more than \$6 million to respond and recover. In Texas, the computer systems of 22 small towns were simultaneously hacked, locked down, and held for ransom in a coordinated effort by a single actor in late August.

It is estimated that more than two-thirds of ransomware attacks targeted state and local governments in 2019. Ransomware has become so prevalent that experts now view it as its own economy, where hackers advertise their services and customers provide ratings and even review the criminal’s customer service. As a result, ransomware and cybersecurity threats in general are now high on every municipality’s list of risks that must be addressed.

## Ransomware and the Evolving Landscape of Threats

What is ransomware, and what can municipalities do to respond to it and other cyber threats? When your computer slows down, is running poorly, or is effected by malicious software, you might refer to the problem as a “virus.” A virus is actually one of several types of “malware.” Malware is a catch-all term for malicious software, regardless of how it works. There are more types of malware than we could hope to cover here, including viruses, spyware, adware, trojans, worms, and yes, ransomware. Some types of malware sit in the background and work discretely by, for example, collecting sensitive information on a computer system and sending it to the hacker. Others inflict an obvious, overt effect. Although ransomware comes in several varieties, it is often a hybrid that initially works in the background, and then reveals itself.

Ransomware can infect a municipality’s computer system in many ways. An employee might click a link or open an attachment in an email that appears to be trustworthy (“phishing”). They might visit a malicious website. Or, a criminal might use a more aggressive tactic targeting security flaws to install ransomware. After ransomware is installed on a system it will usually begin locking down (“encrypting”) the system’s files immediately, making them inaccessible. The ransomware will then show a screen informing the user that the system’s files will continue to be inaccessible unless the ransom is paid. The ransom typically requires payment in

the form of Bitcoin—a now infamous digital currency that is difficult to trace to its owner. Ransomware commonly includes a countdown timer coupled with language threatening to increase the ransom amount if the timer reaches zero.

The effected municipality’s security sometimes identifies and stops the ransomware before it encrypts a significant amount of the system’s files. The municipality might also be able to replace the encrypted files with backup copies. However, it is all too common that ransomware avoids detection, and backups are not available either because the malicious actor targeted them, or because the computer system’s backups are unavailable, insufficient, or even nonexistent.

Ransomware can hold services hostage, too. For example, in January 2019, just as a snowstorm hit Northeast Ohio, an Akron 311 service designed to let residents know when their streets would be cleared was taken down by ransomware.

## To Pay or Not to Pay

When ransomware is successful, the victim municipality is faced with a difficult decision. The hottest topic when it comes to municipal ransomware has been whether to pay the ransom. Historically, law enforcement experts like the Federal Bureau of Investigation and IT experts have recommended not paying. Paying the ransom involves several risks. The criminal might demand additional payment, return the files in a corrupted or disorganized state, or refuse to return them altogether. The criminal might also attempt to re-infect the

municipality. Recognizing these risks, and hoping to diminish the broader “ransomware economy,” more than 225 prominent U.S. mayors signed a resolution not to pay ransoms to hackers during the 2019 annual meeting of the U.S. Conference of Mayors. Nonetheless, the most public examples of municipal ransomware continue to show mixed results. For example, none of the 22 Texas municipalities mentioned above paid in 2019, but several in Florida did. It can feel overwhelmingly costly or even impossible to recreate the encrypted files or effected systems.



“...ransomware and cybersecurity threats in general are now high on every municipality’s list of risks that must be addressed.”


## How Can Municipalities Address Cybersecurity Risks?

Municipalities should consider their preparedness for ransomware and other types of cybersecurity threats like those designed to provide a hacker with unauthorized access to sensitive information. A reasonable approach to information security involves a multi-layered approach with technical and procedural measures to prevent cybersecurity incidents and minimize their impact when they do occur.

Regarding non-technical measures, a municipality should ask the following questions when considering its cybersecurity posture:

- Do we have an incident response plan? Is it updated and practiced?
- Have we identified a team of people (IT, legal, public relations, etc.) who will respond to an incident? How will our team make important decisions?
- Do we have cyber insurance coverage, and what does it cover?
- Do we require our third-party vendors to maintain adequate security measures and notify us of a data security incident? Do we understand our contractual obligations to third parties if we are a victim of an incident?
- Are we regularly reviewing internal and external security risks and implementing measures to mitigate or eliminate them?
- Do we offer periodic employee training on security best practices?
- Regarding technical measures, a municipality should consider the following protections:
  - Limit administrative privileges
  - Multi-factor authentication and strong password rules
  - Allow users to access only the information that is necessary for their role
  - Data mapping to inventory where information is stored
  - Penetration testing and vulnerability assessments
  - Encryption

- Regular and enforced patching and updating
- Network activity monitoring
- A strong data retention and minimization policy that is used

Finally, municipalities should recognize that cybersecurity threats will continue to evolve. Therefore, it is essential to implement best practices that will allow your municipality to adapt to the constantly changing landscape of threats. 

---

*Taylor Gast is an attorney with Foster Swift Collins & Smith who regularly helps clients identify and respond to cybersecurity risks. He can be reached at 517.371.8238 or [tgast@fosterswift.com](mailto:tgast@fosterswift.com).*