# Local Governments Are Under Attack

## Hackers commonly breach municipal IT systems

**by Sandy Reeser**
**VC3**



Can you imagine how more than 600,000 residents would feel about not being able to call an ambulance, a fire truck or a police officer? That happened in Baltimore when its 311 and 911 systems were hacked in 2018. The city lost its 311 and 911 services for 17 hours.

Also in 2018, Atlanta, a city with almost half a million people, was without many city services for a week due to hacking. Police were handwriting reports of crimes. The courts were backlogged. People couldn't pay their municipal bills. Even more recently, in March 2019, Jackson County, Ga., paid $400,000 in ransom to hackers to recover its encrypted data.

These cyber incidents not uncommon. Local government has become one of the top hacker targets. Many cities are attacked every day, and some of them are attacked on an *hourly* basis, according to the ICMA Cybersecurity Research Report. (To access the information in the report, go to *icma.org/documents/cybersecurity-survey-snapshot*.)

Municipalities face two significant challenges in fighting this battle.

First, unlike commercial businesses, local governments are required by law to publish a lot of information about their daily operations. This requirement is certainly positive from the perspective of transparency to your citizens, but unfortunately, it also provides hackers with information that they can exploit to gain access to your data and your cash.

Additionally, most local governments cannot afford to hire full-time security experts, and current staff are not equipped or have the time to become security experts or to maintain a working knowledge of this rapidly changing landscape.

No city is immune. Most hacking attempts go undetected unless the hackers deliberately set out to make their feat obvious. Breaches sometimes aren't discovered for months.

Many cities are stuck with aging infrastructure, outdated software and ancient technology, along with weak security policies and limited budgets. They are fighting a battle against hackers who are incredibly skilled in their field, possess the latest hardware and technology, and are determined to demonstrate their computer prowess in the most extravagant fashion possible. Many more hackers are in it strictly for the money.

### PROTECTION FROM HACKERS

Your email system is a prime target for attack. The following steps will help you protect it from hackers.

**Educate your employees.** Employees shouldn't open any attachment that isn't expected or isn't from a known source. If there is anything suspicious about it, they should call the sender and ask if he or she sent it or contact their technology staff person.

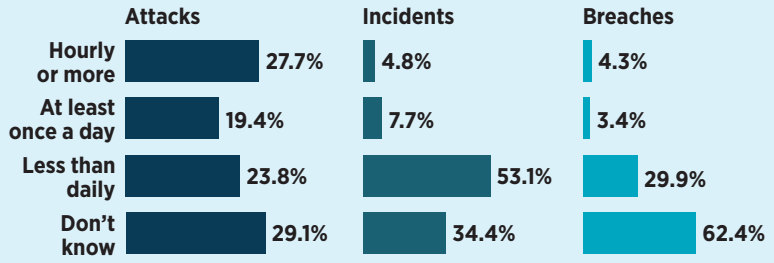
**Incorporate anti-spam filtering on your email system.** Anti-spam filtering will rid your system of most of the threats, but filtering is meant to supplement the education of your workers. You must teach employees not to assume that everything in email is safe.

**Have up-to-date software.** Even if you have the latest operating system, it is essential that regular updating and patching is performed to ensure your system stays secure and minimizes your exposure to hackers.

The security of your software and email are only part of the equation. If you believe your city needs outside assistance, consider engaging with a technology partner that specializes in local government security analysis.

Sandy Reeser is CEO of VC3 Inc., an IT services and computer consultant. For more information, call Christie Williams with VC3 at (404) 790-3885. QC

### ICMA REPORTED ATTACK RATES




Attacks are attempts to gain unauthorized access to cause mischief or do harm. Incidents are events that compromise confidentiality, integrity or availability of a computer system. Breaches are incidents that result in confirmed disclosure of information to an unauthorized person.

**Source:** 2016 Cybersecurity Survey conducted by ICMA, the International City/County Management Association, and the University of Maryland, Baltimore County.