CYBERSECURITY:

Ransomware Protection for Cities

JA | JAMES ALLEN INSURANCE

What is Ransomware?

YOUR CITY'S COMPUTERS HOLD VALUABLE INFORMATION. ARE YOU SURE YOUR FILES ARE SECURE?

Ransomware is a form of malware. It encrypts files, making them unusable and unreadable. Hackers then ask for a ransom in exchange for the decryption key that will restore your files.

Ransomware enters your network through anything from an email attachment to a USB drive. Typically, the malicious software starts encrypting files on local computers and networks before the victim knows it is happening. It is downloaded and installed without the user's knowledge, hidden among the computer's ordinary files and operations. Once files are encrypted, a ransom note will then pop up on the user's screen, threatening destruction if a payment is not made.

Hackers don't always go after the average Joe. They like to target government entities—cities, schools, police stations, etc. Hackers have proven these are easy targets with large pocketbooks and a lot to lose.

The FBI reports more than $1 billion was paid to ransomware hackers in 2016.

The Cost of a Ransomware Attack

Ransomware attacks can be very expensive. Ransoms can range anywhere from a few hundred dollars—if you're lucky—up to hundreds of thousands of dollars. The FBI reports more than $1 billion was paid to ransomware hackers in 2016. The Department of Justice reports an average of 4,000 attacks per day in the U.S. that same year.

And it's not just the ransom that has to be paid. The aftermath can cost even more. Recently, Atlanta incurred a $17 million loss while having to rebuild infrastructure and recover lost data. Baltimore experienced a similar situation, costing the city $18 million. Is that a price you and your taxpayers are willing to pay?

Attacks on the Rise

Since 2013, at least 170 county, city and state government systems have been hacked. And that number is quickly rising. According to McAfee, ransomware attacks have more than doubled in 2019. Intrusion of data and damage to our way of life are happening across the nation—and in our own backyard, too. In 2019, LaPorte, Ind., paid hackers over $130,000 after the city's computer network, website and email systems were compromised. Lake County and Evansville, Ind., have also been hit hard.

CITIES THAT HAVE BEEN UNDER ATTACK:

August 19, 2019: 22 Texas towns

July 24, 2019: State of Louisiana

June 26, 2019: Lake City, Florida

June 20, 2019: Riviera Beach, Florida

May 7, 2019: Baltimore

April 2019: Cleveland Hopkins International Airport

April 2019: Augusta, Maine

April 2019: Tallahassee, Florida

March 2019: Albany, New York

March 2019: Jackson County, Georgia

March 2018: Atlanta

February 2018: Colorado Department of Transportation

According to McAfee, ransomware attacks have more than doubled in 2019.

No City is Safe

In 2019, 55 ransomware attacks on state, county and local governments have taken place thus far. Of those, 38 were on local governments, 14 were on county governments, and three were on state governments. Nearly half of the government victims were small municipalities with populations of 50,000 or less, and 24% had fewer than 15,000 residents.

How Cities are Affected

When cities are under a ransomware attack, every minute counts. While negotiations are underway and heart rates rise, the city itself is compromised. Operations are halted. Records from criminal to medical cannot be accessed, transportation such as airports and bus systems are a mess, and even phones are offline. The impact is not only felt financially but also within the daily operations of a town or city—both during the attack and the time it takes to make repairs.

Tier 1 Cities

CITIES COMPARABLE IN SIZE TO CHICAGO

- Major transportation backup
- Loss of computers could destabilize major infrastructure necessities
- Policing becomes almost impossible with limited access to databases

Tier 2 Cities

CITIES COMPARABLE IN SIZE TO INDIANAPOLIS

- Transportation system works slowly/offline
- Ticketing/parking kiosks are inoperable
- All tickets and database entry must be done by hand and on paper
- Amenities can be extremely difficult or impossible to track

Tier 3 Cities

CITIES COMPARABLE IN SIZE TO BEDFORD, IND.

- Ticketing services and utility payment systems go offline for an extended period of time
- Costs to repair or rebuild network infrastructure could exceed all funds available in the budget

By Marc Graber

Marc Graber has been in the insurance industry for 34 years, and currently serves as Director of Asset Management & Retail for James Allen Insurance. In that role, he oversees the agency's cybersecurity service line where he helps organizations achieve peace of mind that they will be covered in the event of a cyber attack.

How to Prepare

INVEST IN CYBERSECURITY INSURANCE

Select an insurance policy that takes a comprehensive approach to cybersecurity and supports your city's compliance requirements and risk management systems.

LOCK ADMINISTRATIVE RIGHTS

Limit the number of users with permissions on your server. This can limit the spread of a ransomware attack throughout the network.

STAY UP TO DATE

Keep your system up to date with the latest patches and security measures. Reducing vulnerability in applications and operating systems in turn reduces the likelihood of an attack.

BACK UP DATA

Back up your data daily to a local storage device or server that is offline. This prevents the ransomware from being able to reach it.

DON'T OPEN ATTACHMENTS

If an email seems suspicious, it probably is. When you don't recognize a sender or the message asking you to open an attachment seems unusual, do not open it. This also goes for online ads. Being cautious also protects your computers from malware. A new tactic includes "malvertising," where ads are embedded with malware and then sent out to sites you know and trust.

MONITOR YOUR SERVER AND NETWORK

Monitoring tools can detect any unusual files that might otherwise be overlooked. This prevents malware from starting an attack.