Local Government Cyber Roundup: Disruptions, Data Breaches, Financial Loss

Jan – Jun 2019

Disruptions

A **phishing email led to ransomware** for the city of Riviera Beach, which shut down email and computer systems. The city council **authorized a $600,000 ransom payment** in bitcoin to unlock their systems and data.

Riviera Beach, FL / Jun 2019 / Story

Lake City **computer systems, including email system, and phone systems were shut down** by ransomware. After struggling to recover their systems, they agreed to **pay almost $500,000 in ransom.**

Lake City, FL / Jun 2019 / Story Follow-up

A virus infected Philadelphia's online court system, **shutting down the system for four weeks.**

Philadelphia, PA / Jun 2019 / Story

A phishing attack spread a virus that caused a shutdown of Luzerne County courthouse servers and workstations that lasted days.

Luzerne, PA / May 2019 / Story

For the second time in just over a year, the city of Baltimore has been hit with ransomware, forcing the city to shut down the majority of its servers.

Baltimore, MD / May 2019 / Story

A ransomware attack shut down the Daviess County Public Library for three days to restore systems and take inventory.

Daviess, KY / May 2019 / Story

Stuart city took weeks to recover after **falling victim to a phishing scam,** leading to **malware that froze the city's servers.** A bitcoin ransom was demanded, but the city refused to negotiate.

Stuart, FL / Apr 2019 / Story

The City of Augusta was **shut down for four days by a ransomware attack.** Computers used by public safety officials were also shut down by the virus.

Augusta, ME / Apr 2019 / Story

Garfield County went **weeks without access to its systems** due to a ransomware attack. It eventually paid a bitcoin ransom to restore access to their systems.

Garfield, UT / Apr 2019 / Story

A phishing attack led to ransomware for the city of Greenville. The city's operations were halted or slowed for over two weeks as the city worked to recover their data.

Greenville, NC / Apr 2019 / Story

Genesee County was hit with ransomware and their **systems were affected for nearly a week.**

Genesee, WA / Apr 2019 / Story

For the third time in six years, the Orange County network was **infected with ransomware. Services were shut down for days.**

Hillsborough, NC / Mar 2019 / Story

Fort Collins Loveland Water District and South Fort Collins Sanitation District had to **shut down operations for three weeks after a ransomware attack,** which was the second attack in two years.

Fort Collins, CO / Mar 2019 / Story

Data Breaches

A breach of the Borough of Westwood, NJ exposed **names, social security numbers, driver's license numbers or state identification numbers, or financial account or credit/debit card information** to an unauthorized third party.

Westwood, NJ / Jun 2019 / Story

A **software vulnerability may have allowed a data breach** that compromised customer information at Lewes Public Works. Information included **names, email addresses, payment card information, and other financial information.**

Lewes, DE / Jun 2019 / Story

An **unauthorized person gained access** to sensitive information belonging to employees and customers of Broome County. Information includes **names, contact information, social security numbers, bank accounts or financial information, dates of birth, medical record numbers, patient identification numbers, medical or clinical information, health insurance and claims information, and credit card information.**

Broome, PA / Jun 2019 / Story

The information of over **3,000 Edcouch residents was stolen** and **$40,000 in bitcoin** was demanded by the hacker.

Edcouch, TX / Jun 2019 / Story

The County Administrator at Lauderdale County **accidentally shared via e-mail** the private information of **over 100 employees.** Data included **names, social security numbers, and phone numbers.**

Lauderdale, MS / Apr 2019 / Story

A Dakota County **employee's email was hacked, compromising current and former clients' personal information.** Information included **names, addresses, driver's license numbers, social security numbers, health insurance information, and/or medical history, treatment, or diagnoses information.**
Hastings, MN / Apr 2019 / Story

A phishing attack led to the compromise of Thomas County School District's online banking system. Employee payroll information such as names, employee ID numbers, bank account numbers, and bank routing numbers.

Thomas, GA / Mar 2019 / Story

Pasquotank-Camden Emergency Medical Services had over **40,000 medical records compromised** due to a **vulnerability in the county's billing software** which is managed by a **third-party vendor.**

Pasquotank, *NC / Feb 2019 / Story*

Hackers **gained access to payment information** for close to **4,000 residents** through a **third-party bill processing company.**

Pompano Beach, *FL / Feb 2019 / Story*

Financial Loss

The **third-party vendor** that hosts payroll for the city of Tallahassee was **hacked and paychecks worth $500K were diverted.**

Tallahassee, FL / Apr 2019 / Story