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

Jul – Dec 2018

Disruptions

The Onslow Water and Sewer Authority's **internal computer system was hit by a ransomware** attack **crippling their network for weeks.** A ransom notice was given, but the Authority refused to pay.

Jacksonville, NC / Oct 2018 / Story

Madison County experienced a ransomware attack that **affected operations for nearly a week.** County **employees were unable to send or receive email or access network files.** A demand for ransom was denied by the county.

Madison, ID / Oct 2018 / Story

Anne Arundel County Library **computers were hit with the Emotet virus,** causing officials to take library **computers out of service** and asking users to **monitor their accounts for fraud.**

Anne Arundel, MD / Oct 2018 / Story

A **virus shut down internet and phone operations** for several departments in Beatrice for days.

Beatrice, NE / Sep 2018 / Story

Coweta County, GA network was hit with ransomware and shut down all servers as a precaution. The county did not pay the 50 bitcoin (~$341,000) ransom.

Coweta, GA / Aug 2018 / Story

Data Breaches and Disclosures

A data breach affected **4,600 customers** using the **city's parking ticket payment system. Click2Gov** was the vendor.

Ames, IA / Dec 2018 / Story

The city of Lake Charles is investigating unauthorized access to its network.

Lake Charles, LA / Dec 2018 / Story

Wage reports containing **employee names and social security numbers** were found wadded up in an Indianapolis man's backyard.

St. Joseph, IN / Dec 2018 / Story

An employee sent out a spreadsheet with hidden columns that **contained the Protected Health Information (PHI)** of 1350 employees.

Butler, OH / Dec 2018 / Story

The City of Topeka had **10,000 online bill pay customers** affected by a **security risk with third party vendor Click2Gov. Credit card information** was potentially compromised.

Topeka, KS / Dec 2018 / Story

Hackers **gained access** to Ramsey County Social Services employee accounts in **an attempt to divert their paychecks.** Through this breach, it was determined that **500 clients' personal information, such as social security numbers, dates of birth, addresses, and health information, may have also been compromised.**

Ramsey, MN / Dec 2018 / Story

A Wright County **employee downloaded data to his home computer** to work at home, **compromising PII of 72,000 residents.**

Wright, MN / Dec 2018 / Story

The City of Bakersfield had 2,400 **online bill pay customers** affected by the **Click2Gov security issue.**

Bakersfield, CA / Nov 2018 / Story

Three employees of the Town of Christiansburg had their **accounts compromised due to phishing.**

Christiansburg, VA / Oct 2018 / Story

The City of Lake Worth utility customers were affected by the **Click2Gov security issue.**

Lake Worth, FL / Oct 2018 / Story

The Indio Water Authority's customers were affected by the **Click2Gov security issue.**

Indio, CA / Oct 2018 / Story

Bossier City **online bill pay customers** were affected by the **Click2Gov security issue.**

Bossier, LA / Aug 2018 / Story

Adams County **network was breached** with hackers accessing personal data of 250,000+ people. Data included **names, addresses, birthdates, social security numbers, license numbers, fingerprints, and even full face photos.**

Adams, WI / Aug 2018 / Story

Social security numbers were inadvertently included on arrest warrants that were **published publicly**

on the Davidson County Criminal Court Clerk's website.

Davidson, TN / Aug 2018 / Story

Employees of the City of Amarillo had their data put at risk when a third party auditor **lost an encrypted flash drive** containing **names, addresses, bank deposit information, dates of birth, and social security numbers.**

Amarillo, TX / Nov 2018 / Story

Hackers phished Hennepin County employees, **stole their credentials, and used their accounts to send out malicious email.**

Hennepin, MN / Aug 2018 /Story

Financial Loss

In addition to **staff credentials being breached,** the Galloway Township was **defrauded of $200,000 in falsified wire transfers.**

Galloway Township, NJ / Nov 2018 / Story

New Haven city officials **paid more than $2,000 in bitcoin** to unlock 23 servers and restore access to city data.

New Haven, CT / Oct 2018 / Story