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

Jan – Jun 2017

Disruptions

A **ransomware attack** forced Mountain Home water department to **move operations to paper for three days** while the system was restored.

Elmore, ID / *Mar 2017* / *Story*

Every department in Bingham County **was affected by a ransomware attack. Phone and computer systems, including a back-up system, were affected** by the attack which **disrupted operations for at least three days.**

Bingham, ID / *Feb 2017* / *Story*

Over 1,000 Licking County computers were shut down due to a **malware attack,** affecting the operations of many departments for **at least four days.**

Licking, OH / *Feb 2017* / *Story*

Every public computer in the St. Louis Public Library system **was infected, preventing all book borrowing and cutting off internet access** to those that rely on it.

St. Louis, MO / *Jan 2017* / *Story*

Data Breaches

The Township of Springfield in New Jersey found **suspicious activity** on their police department management server **which included full names, driver's license or state card identification numbers, birth dates, addresses, and telephone numbers.**

Springfield, NJ / *Jun 2017*/ *Story*

Names, addresses, and social security numbers of tens of thousands of Cameron County residents were found on a server sold at a flea market. A **law enforcement database** with **names, addresses, VIN numbers, and Social Security numbers** was also found on the server.

Rio Grande, TX / May 2017 / Story

An **unauthorized party had access to a City of Stillwater computer for 22 days.** Personal information such as **names, addresses, driver's license numbers, and social security numbers** were stored on the computer.

Stillwater, OK / *May 2017*/ *Story*

Officials from the Larimer County Clerk and Recorder's office **published sensitive information belonging to thousands of people to an online portal for months.** Sensitive information included **child support liens, death certificates, and commercial lending filings, many which included social security numbers and birth dates.**

Fort Collins, CO / *May 2017*/ *Story*

Mecklenburg County **officials mistakenly gave information to two media outlets HIPAA protected information** to news media outlets.

Mecklenburg, NC / *Mar 2017*/ *Story*

A payroll administrator from Sebastian County **sent an e-mail** to a group of employees **containing links to approximately 200 employees' bank account numbers and routing numbers.**

Sebastian, AR / Mar 2017 / Story

A **data breach** at Warren County Sheriff's department **exposed thousands of sensitive records online, including jail incident reports, arrest records,** and more. The Sheriff's department also fell victim to a ransomware attack last year.

Warren, MO / *Mar 2017* / *Story*

According to the San Luis Obispo County Clerk-Recorder's Office**, twelve people, including 10 San Luis Obispo County residents, were notified that their Social Security numbers were "inadvertently" released to two private title companies** because of a technical error.

San Luis Obispo, CA / *Mar 2017* / *Story*

A **Multnomah Health Department employee automatically forwarded all emails received** in the employee's county email account **to a personal Google email account**. E-mails forwarded **included PHI and HIPAA information.** The **breach was not discovered for four years.**

Portland, OR / *Jan 2017* / *Story*

The Cockrell Hill **Police Department lost video evidence and a cache of digital documents** that was not backed up after a ransomware attack**.**

Dallas, TX / *Jan 2017* / *Story*