

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

Jul – Dec 2017

Disruptions

It was discovered that **3,700 residents had their information compromised** after a server for **Tom's River police department malfunctioned and would not start when rebooted.**

Tom's River, NJ / Aug 2017 / [Story](#)

The city of Oceanside was **forced to shut down its online bill payment system after 25 residents reported unauthorized charges on credit cards** used to set up their bill pay accounts.

Oceanside, CA / Aug 2017 / [Story](#)

Data Breaches

Over **700 patients had their information put at risk** when a contractor for the Cook County Health and Hospitals System had their system breached. Data included **patient names, medical record numbers, dates of birth, and account numbers.**

Cook County, IL / Nov 2017 / [Story](#)

A **third party payment system for Midland County, TX was breached**, possibly putting resident information in jeopardy.

Midland County, TX / Sep 2017 / [Story](#)

A **laptop containing sensitive information was stolen** out of a San Francisco District Attorney's car.

San Francisco, CA / Oct 2017 / [Story](#)

A **computer containing names, addresses, and polling places** of Charlottesville and Albemarle County residents **was lost**. Upon further inspection, **a second computer has been missing since 2015.**

Charlottesville, VA / Sep 2017 / [Story](#)

Erie County's Office of Children and Youth had resident **children's personal information put at risk** when a **third party vendor experienced a data breach**. Information exposed includes **names, dates of birth and Social Security numbers.**

Erie, PA / Jul 2017 / [Story](#)