K-12 Cyber Roundup: Disruptions, Data Breaches, Financial Loss

Jul – Dec 2018

Disruptions

A Mount Zion School District **student used a distributed denial of services attack to shut down the district's website.**

Mount Zion, IL / Dec 2018 / Story

Johannesburg-Lewiston Area Schools were hit with **ransomware and used their insurance to pay the ransom demand.** The **network was affected for over a week.**

Johannesburg, *MI / Nov 2018 / Story*

Chesapeake Public Schools was hit with **ransomware through a phishing attack, affecting technology in classrooms and school Wi-Fi.**

Chesapeake, *VA / Nov 2018 / Story*

The Oklahoma City Public School District was **affected by a denial of service attack** on a third party vendor that **limited access to one of their portals.**

Oklahoma City, OK / Sep 2018 / Story

The Monroe County School District had to **shut down their network for three days** because of a **ransomware attack** named GandCrab.

Monroe, FL / Sep 2018 / Story

Cloquet School District was hit with a **ransomware attack** for the second time in two years and expected to **cost the district $15,000 in insurance deductibles.**

Cloquet, MN / Aug 2018 / Story

Data Breaches and Disclosures

A phishing-related breach compromised the personal information of up to **500,000 current and former students and staff** from the San Diego Unified School District**. Birth dates, social security numbers, addresses, and phone numbers are among the exposed data.**

San Diego / Dec 2018 / Story

Current and former staff members at AOS 77 in Washington County were alerted of a **data breach that included their dates of birth, addresses, and social security numbers.**

Washington, ME / Dec 2018 / Story

Over **150 students and employees** of Norfolk schools had their **medical information and cell phone numbers shared publicly.**

Norfolk, VA / Oct 2018 / Story

Students at Honeoye Falls-Lima School Central District **stole the superintendent's login credentials to breach the school's computer system.**

Monroe County, NY / Oct 2018 / Story

Two thousand DC Public Schools students had their personal information mistakenly **published online and publicly accessible for six months. Information included student names and birthdates.**

Washington, DC / Sep 2018 / Story

Crisis plans containing **student medical information and floor plans** of three schools **were posted publicly** on the Norfolk Public Schools website**.**

Norfolk, VA / Aug 2018 / Story

The **confidential records** of former Tulsa Public Schools students were **found in a dumpster** behind a local elementary school**, violating FERPA.**

Tulsa, OK / Aug 2018 / Story

Financial Loss

The Henderson ISD initiated a **$600K electronic payment to a fraudulent vendor** in a scheme known as **Business Email Compromise (BEC).**

Henderson, TX / Oct 2018 / Story