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

Jan – Jun 2019

Disruptions

Oklahoma City Public Schools was **compromised with malware,** facing **both disruptions in email services and deletions of data.**

Oklahoma City, OK / *May 2019* / *Story*

Sugar-Salem School District 322 was hit with **ransomware, causing them to shut down all online access for two days.**

Sugar City, ID / Apr 2019 / Story

Taos Municipal Schools suffered a **ransomware attack** that affected **email, classroom instruction, and the district website.** It took a month to get their systems back up and running.

Taos, NM / Mar 2019 / Story

The Newport School District was hit with a **phishing attack** that led to a **disruption that lasted two to three weeks.**

Newport, PA / Mar 2019 / Story

Mount Zion School District experienced a **network disruption for the second time** in a few months, this time due to a **ransomware attack by a foreign hacker.**

Mount Zion, IL / Feb 2019 / Story

Data Breaches

Names, dates of birth, and social security numbers of 7,000 students were compromised when a **staff member's account was hacked.**

Hopkins, KY / Jun 2019 / Story

An employee transferred student information for several thousand students to a personal email account.

Jefferson City, MO / May 2019 / Story

Paterson Public Schools experienced a major data breach with more than **23,000 usernames, passwords and other login credentials stolen.**

Paterson, NJ / May 2019 / Story

The San Francisco Unified School District alerted families of **current and former students** at Buena Vista Horace Mann that their students' data was shared with non-District personnel.

San Francisco, CA / Apr 2019 / Story

A **data entry error** exposed the **names, addresses, grade point averages and college entrance exam scores of nearly two dozen students** to users other than their parents.

Arlington, VA / Apr 2019 / Story

Employees of the Carmel Unified School District fell for a **phishing scam** and compromised personal information of other District employees. Personal information included **social security numbers of employees and their spouses and children, marriage and birth certificates, and doctor's notes.**

Carmel, CA / Mar 2019 / Story

The Thomas County School District network was **breached by hackers** who **obtained employee payroll information, including bank account numbers.**

Thomas, GA / Mar 2019 / Story

Worcester School Department **gave a third-party vendor the last four digits of teachers' social security numbers to use as a password.**

Worcester, MA / Mar 2019 / Story

Four high school students **breached the Dickinson High School computer system to change grades.**

Jersey City, NJ / Feb 2019 / Story

A Centinela Valley Union High School District **employee was phished for employee W-2s,** which include sensitive information like **names, addresses, social security numbers, and wage information.**

Lawndale, CA / Feb 2019 / Story

Student test scores were accidentally emailed to all parents at Hallsville Elementary School.

Manchester, NH / Feb 2019 / Story

Financial Loss

An **undisclosed amount of money has been compromised due to a cyberattack** at Aurora City Schools.

Aurora, OH / Mar 2019 / Story

Jackson County paid over $400,000 to hackers to decrypt their network after a ransomware attack.

Jackson, GA / Mar 2019 / Story

Scott County Schools learned it had **fallen victim to a vendor payment phishing scam** after a vendor reported non-payment. The District **lost $3.7 million.**

Georgetown, KY / Apr 2019 / Story