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

Jul – Dec 2017

Disruptions

Flathead, Montana school district fell victim to a multipronged cyber-attack that included threatening text messages to staff, students, and parents and ransom demands. These **threats forced school closures for four days that affected 30 schools and 15,000 students.**

Flathead, MT / Sep 2017 / Story

Data Breaches

Names, student numbers, and GPAs of current Palo Alto High School students were **shared on a third party website after an unknown breach.**

Palo Alto, CA / Oct 2017 / Story

Two students from United ISD placed a **keylogging device on several educators' computers to access files and change grades.**

Laredo, TX / Aug 2017 / Story

An **accidental release** of information via email attachment compromised over **9,000 students.** Information included **names, grades, identification numbers, email addresses, mailing addresses, phone numbers, bus routes, pick up and drop off times, pick up and drop off locations, and schools of attendance.**

South Washington, MN / Aug 2017 / Story

Over **4,000 students had private information shared with parents and fellow students** due to an **accidental release** by a school employee.

Sanford, FL / Aug 2017 / Story

Personal information of **at least 53 employees, retirees, and dependents** of Fresno Unified School District was discovered years after the data was stolen. Information included **names, addresses, birthdates, phone numbers, and social security numbers.**

Fresno, CA / Jul 2017 / Story

Financial Loss

Dorchester School District 2 paid a **$2,900 ransom** to have the data on 25 servers decrypted after a ransomware attack.

Dorchester, SC / Aug 2017 / Story