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

Jul – Dec 2016

Disruptions

Bigfork School District's computer systems **were infected with ransomware, locking finance, personnel, and student records.**

Bigfork, MT / Nov 2016 / *Story*

Data Breaches and Disclosures

A Chesapeake Public Schools **employee's laptop was stolen.** The laptop contained **names, social security numbers, and bank account information** for over **10,000 employees.**

Chesapeake, VA / *Dec 2016* / *Story*

A Chicago Public Schools **employee improperly provided the names, addresses, and schools of 30,000 students** to a Noble Network of Charter Schools who used the information to market to students.

Chicago, IL / *Nov 2016* / *Story*

An employee of Katy Independent School District **accidentally uploaded PII of employees and students** to a software application. No hacking was involved, however personal information was not properly protected.

Katy, TX / *Oct 2016* / *Story*

A group of high school students at Upper Arlington High School were able to **hack into an active student directory** and see privileged student information.

Upper Arlington, OH / *Oct 2016* / *Story*

A representative who works at La Joya American Federation of Teachers **accidentally sent out an email** containing the social security numbers and payroll information of **1,600 La Joya ISD** teachers.

La Joya, TX / *Sep 2016* / *Story*

Financial Loss

The business manager for East Baton Rouge Parish school system **fell victim to a phishing scam** that ended with her **wiring $46,500** to someone impersonating the school system's superintendent.

East Baton Rouge Parish School System, LA / Nov 2016 / Story