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

Jan – Jun 2017

Disruptions

The network servers for Confluence Charter Schools in St. Louis were hacked in April. The hacking affected the schools' **emails, phones, student information system and payroll system, with some files made unrecoverable.**

St. Louis, MO / Apr 2017 / Story

A hacker used **malware to infect the school's computers,** forcing students, teachers and administrators at Pekin Community High School to **forgo their computer systems.**

Pekin, IL / Apr 2017 / Story

Student and teacher records from Forsyth Public Schools were **corrupted** when their systems were hit with **malware.** Student data, stored in a third party management system, was retrievable. However **teacher data, stored on the district's servers, was unrecoverable** at the time the article was printed.

Forsyth, MT / *Mar 2017 / Story*

Internal documents were left encrypted and inaccessible after a ransomware attack on Kanawha County Schools.

Kanawha, WV / Jan 2017 / Story

Data Breaches

A Niskayuna Central School District **employee's laptop was stolen.** The laptop contained **names, dates of birth, and addresses** for almost **1,000 students.**

Niskayuna, NY / *May 2017 / Story*

Due to **a software malfunction of third party software, PII** of approximately **600 Mt. Diablo Unified School District students** was exposed. Accessible information included **addresses, home phone numbers, immunization records, required medication, medical history, grades, class schedules, test scores, parent email addresses, attendance records, and transcripts.**

Concord, CA / *Apr 2017 / Story*

A **third party vendor's software was hacked, exposing user names, encrypted passwords, and e-mail addresses of over 33,000** current and past Williamson County Schools' students. This breach has affected multiple school districts using this vendor's software.

Williamson, TN / *May 2017* / *Story*

Thousands of employees became potential victims of tax fraud when a Tipton School **employee emailed a PDF document containing W-2s of school employees to someone posing as the Director of Schools.**

Covington, TN/ *Jan 2017* / *Story*

About **3,300 Greenwood School District 50 employees and their dependents** had personal information compromised after an **unauthorized user accessed employee emails as well as current and former employee payroll accounts. W-2s were compromised in the breach.**

Greenwood, SC / *Apr 2017* / *Story*

Some **employees of Cleveland Metropolitan School District fell victim to a phishing scam** that **stole their login credentials.** Information accessible to the scammer included **name, Social Security number, driver's license number, medical record number, and/or medical history.**

Cleveland, OH/ *Apr 2017* / *Story*

Personal employee information including **job title, salary, home address, Social Security number, employee number, and work location,** was **accidentally emailed** to over **2,000 Sunnyside Unified School District employees.** Tuscon, AZ/ *Mar 2017* / *Story*

The South Washington County **school district's server was hacked by a student.** Over **15,000 records with student names, Social Security numbers and addresses were stolen.**

Cottage Grove, MN / *Feb 2017* / *Story*

Confidential information on Chicago Public Schools students, including **medical conditions and dates of birth,** were stored on **unsecured websites accessible by the public.** Over **1,600 records** were found, dating back to 2013.

Chicago, IL/ *Feb 2017* / *Story*

Odessa School District's employees' personal information was breached when someone **pretending to be the superintendent** requested and was sent employees' W-2s.

Odessa, MO/ *Jan 2017* / *Story*

Personal information, including Social Security numbers, of Dracut Public Schools employees **was stolen in a cyberattack.** An employee for what was described as a **sophisticated phishing scheme.**

Dracut, MA / *Jan 2017* / *Story*