K-12 Cyber Roundup: Disruptions and Data Breaches

March – May 2016

School Shutdown

School was canceled for one day while IT admins scrambled to rebuild systems taken over by **ransomware**. The infection spread quickly, even affecting the lunchroom payment system and monitoring for HVAC. Neighboring IT reinforcements were called to help in restoration efforts.

Cloquet School District, MN / March 2016 / Story

Accidental Disclosures

An employee sent copies of fellow employees' health insurance information with **PII to her personal e-mail address** repeatedly. Over 3000 employees affected.

Pulaski County Special School District, AK / March 2016 / Story

A **forgotten backup file containing PII** of around 5000 students and teachers was copied to a flash drive by a former student.

Nazareth Area School District, PA / April 2016 / Story

Roughly 5800 **employee SSNs were sent to a District vendor** due to employee error.

Palm Beach County Schools, FL / May 2016 / Story

Some **36,000 student records** were accidentally disclosed to a public records request in **violation of FERPA**.

Poway Unified School District, CA / May 2016 / Story

Phishing Attacks

Superintendent notifies current and former employees that their PII may have been stolen due to a **phishing e-mail that allowed an attacker onto a workstation** that held the information. School district purchases credit monitoring.

Sequoia Union High School District, CA / March 2016 / Story

Employee **W-2 information** with redacted SSNs and birthdates was sent to an unauthorized third-party as a result of a **phishing e-mail impersonating the Superintendent**. Roughly 55 of the employees reported tax return fraud. Their SSNs were likely obtained from another source.

School Administrative District 4, ME / May 2016 / Story