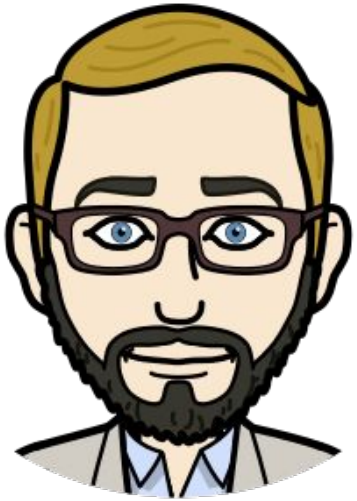
The Human Factor: *Pitfalls in the Management and Use of Technology and How To Limit Liability and Misuse*

Tim Palmatier
General Counsel

OSSEO AREA SCHOOLS
ISD 279



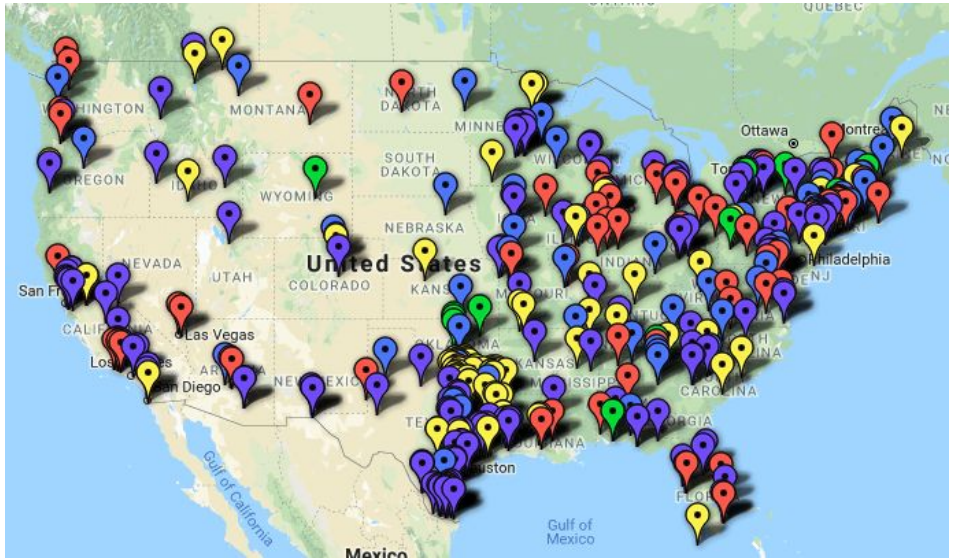
Anthony Padrnos
Executive Director Technology

OSSEO AREA SCHOOLS
ISD 279

Outcome

Participants will explore policies, processes, and procedures to consider for managing user technology access in the school environment

K-12 Cyber Incidents in the News



- 681 Incidents in public schools since January 2016
- 14 in Minnesota

Source: K-12 Cybersecurity Resource Center

"WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

Common Threats to Public Schools

1. Link security (ransomware & phishing emails)
2. Unknown devices
3. Out of date technology
4. User error (staff & student awareness)
5. No backup

Source: Laing (2017)

The Balancing Act

Compliance

PCI, PPRA, FERPA, MGDPA, COPPA, CIPA, HIPAA, Correctional Facilities, State, Local, etc

Attestations

Respected 3rd party attests you meet an agreed upon standard

CoSN Trusted Learning Environment

Digital Citizenship

Ensuring students and staff are protected as they engage with the world online

Security Framework

Best practices to provide appropriate protection

NIST Cybersecurity Framework

Your Cyber Security Program

Customized set of policies, procedures, and SOPs.

Investment of technology and staff based on risks and priorities.

Staff designated to execute security operations, Leaders managing risk and making informed decisions, and situationally aware employees.

Key Starting Areas

- Policies & Procedures
- Access/ Account Management (User Security)
- Asset Management (software & hardware)
- Technology collection & deployment process
- Training (on-boarding and on-going)

NIST Framework

Source: Huergo (2018)


Exposure With Maturity
Opportunistic
Targeted
Risk
Total Exposure
Time

Applicable Laws & Policy Considerations

Laws to be aware of

- FERPA (Family Educational Rights and Privacy Act)
- MGDPA (Minnesota Government Data Practices Act)
- PPRA (Protection of Pupil Rights Amendment)
- Other Laws (Child Online Privacy Protection Act (“COPPA”); Child Internet Protection Act (“CIPA”)

FERPA

- Prohibits the unauthorized disclosure of educational records and personally identifiable information (PII) contained in records.
- The term “education record” is broadly defined to mean “records, files, documents, and other materials” that: (1) “contain information directly related to a student;” and (2) “are maintained by an educational agency or institution or by a person acting for such agency or institution.

FERPA - Provisions Permitting Disclosure without Prior Consent

Directory Information (DI): Technically DI is not a private educational record -- it is information that historically has been regarded as not harmful if disclosed (e.g. student name or address).

School Official Exception: Under the school official exception, schools may disclose PII from students' education records to a provider as long as the provider:

1. Performs a service the district would otherwise provide through its own employees;
2. Meets district definition/criteria for being a **school official with a legitimate educational interest**;
3. Is under the direct control of the district with regard to the use/maintenance of records; and
4. Uses records for authorized purposes and may not re-disclose (unless provider has specific authorization to do so and is otherwise permitted by FERPA).

PPRA

Regulates information that can be sought in student surveys. Absent prior consent of parents, minor students may not be required to submit to a survey, analysis, or evaluation that reveals information about:

- political and religious affiliations or beliefs;
- mental or psychological problems;
- sexual behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of others with whom the student has close family relationships;
- legally recognized privileged or analogous relationships;
- income (except as required by law to determine eligibility)

PPRA

Requires school districts to develop policies outlining PPRA protections which must provide/address:

- Parent's right to inspect, upon the request of the parent, a survey created by a third party before the survey is administered to student;
- Parent's right to opt out of surveys seeking personal information on student;
- Parent's right to inspect instructional material used as part of the educational curriculum for the student;
- The collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose)

MGDPA -- Obtaining Private Data

When attempting to obtain private/confidential data from an individual School District must notify individual of:

- the purpose/intended use of the data;
- whether the individual may refuse or is legally required to supply the data;
- known consequence from supplying or refusing to supply data; and;
- identity of other persons/entities authorized to receive the data

** Requirement commonly referred to as Tennessen Warning*

MGDPA -- Securing Private Data

School District Must:

- Establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected;
- Establish appropriate security safeguards (including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data);
- Ensuring that “not public data” being discarded is destroyed in a way that prevents its contents from being determined

MGDPA -- 3rd Party Contracting

When contracting/using a third party to manage, store or utilize school district data, School District must:

- Require that data on individuals be administered consistent with the MGDPA
- Include contract provision stating that all of the data created, collected, received, stored, used, maintained, or disseminated by the private person/entity in performing functions on behalf of the School District is subject to the requirements of the MGDPA and the person/entity must comply with requirements “as if it were a government entity.”

MGDPA -- Notification of Breach

- School District's are obligated to notify individuals about any unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data
- Requires *written notice* to individuals who are the subject of the private or confidential data for known unauthorized access or reasonable belief of unauthorized access
- Notice of breach must be provided in the most expedient time possible and without unreasonable delay
- Must develop a report (accessible to applicable data subjects) determining the type of data accessed; the number of individuals whose data was accessed; and potentially names/discipline of persons responsible for breach

COPPA- Children's Online Privacy Protection Act

Primarily regulates website provider's online collection of personal information from children under the age of 13

Protects a range of personal information for qualifying minors including: first/last/screen/user names; physical address; phone numbers; social security number; geolocation data; photos/videos/audio files containing child's image or voice; and "persistent identifiers" (tracked cookies);applies to mobile apps and third-party website plug-ins, websites, and some online services.

COPPA- Children's Online Privacy Protection Act

Does not directly apply to schools, however, operators contracted within the school setting must provide notice of their collection activities directly to the school

Schools may consent on behalf of a student if operator collects the child's data *solely for the use and benefit of the school*

Parental consent must be obtained if the operator collects and uses the child's information for commercial purposes

CIPA -- Child Internet Protection Act

Requires that, as a condition of receiving universal service support (i.e. E-Rate funds) a school district must certify that it:

- has and enforces an Internet safety policy; and
- operates/uses a filter on its computers with Internet access

Scenario

Phishing Email

An employee in payroll receives an email from a current employee stating that their bank routing information has changed and they need to update it for their direct deposit. Trying to provide great customer service, the payroll employee responds via email that it can easily be corrected and provides the direct deposit form as an attachment. The payroll employee then receives an email back with a completed form and voided check digitally attached.

If this was your district and the employee email was spoofed, what steps would you take?

Data Incident

A software vendor has just contacted their point of contact (the purchaser list on the PO) in your district via email that they discovered a potential exposure of your student data. This data included student first name, student last name, student ID, and student date of birth. They have provided the point of contact with information regarding what occurred and what steps they took to correct the issue.

How would your district handle this incident?

Lost Laptop

An employee came to your technology department requesting a loaner laptop after their current laptop went missing 4 days ago. After further inquiry by the technology team, this laptop had a spreadsheet on it with student name and special education status identified in it.

How would your district handle this situation?

Ransomware

You come in to your office and log into your office and turn on your computer. When your computer screen comes on the message to the right pops up on your computer. You soon realize that this is happening on all school district computers.

How would your district respond?

Medical Device

A new student has enrolled in your district. This student requires a continuous glucose monitoring system that requires a consistent internet connection. The parents are requesting the use of the district internet for this device to properly function?

How would your district respond to this request?

Questions?

Bibliography

Laing, E. D. (2017, November 28). The top 5 cybersecurity threats for schools. Retrieved August 27, 2018, from https://www.eschoolnews.com/2017/11/29/cybersecurity-threats-schools/

Huergo, J. (2018, April 16). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. Retrieved August 28, 2018, from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

The K-12 Cyber Incident Map. (n.d.). Retrieved October 5, 2018, from https://k12cybersecure.com/map/