SUMMER SCHOOL:

What Pennsylvania School Districts Need to Know About ESSER Relief Funds

Lesson 2: *Data Security & Privacy*

Presenters:

Sandy B. Garfinkel and Stephenie G. Anderson Scialabba

www.eckertseamans.com

July 26, 2021

ECKERT SEAMANS
ATTORNEYS AT LAW

SUMMER SCHOOL: What Pennsylvania School Districts Need to Know About ESSER Relief Funds

Presenters

Sandy B. Garfinkel

Stephenie G. Anderson Scialabba

Jonathan W. Cox

Moderator

Technology Infrastructure Enhancements

- ESSER I

Purchasing educational technology (hardware, software, and connectivity) for students, that aids in the regular and substantive educational interaction between students and their classroom instructors, including low-income students and students with disabilities, which may include assistive or adaptive technology

- ESSER II

Purchase educational technology (including hardware, software and connectivity) for students

- ESSER III

Improving cybersecurity infrastructure

Data Security & Privacy Issues Related to Remote Learning

- COPPA
  - Online collection
- FERPA
  - Electronic records
  - Paper records
- DBLs
  - Electronic records
  - Paper records
- Business Email Compromise
- Ransomware
- Unsecured Email Platforms
- Human Error

Cybersecurity and Remote Learning

With COVID-19, almost every industry, including education, increased use of remote technology tools:

- Video Conferencing
- File Sharing
- Virtual Desktops
- Group Chat
- VPN
- Web-Based Applications & Tools

Cyber Vulnerabilities and Virtual Technology

Consequences of rushed transition from on-site to virtual learning:

- hasty or non-existent policies
- training
- risk assessments
- systems testing
- remote access controls (safe login credentials & multi-factor authentication)

Cybercrime Surge

Clever fraudsters capitalized on chaos and fears surrounding the virus outbreak, enticing individuals to click on links or attachments promising information on disease transmission, treatments and testing. Government program frauds, stimulus program fraud and widespread unemployment compensation scams emerged.

News sources reported an increase in cybercrime ranging from social engineering/credential stealing to ransomware to business e-mail compromise.

COPPA
(Children's Online Privacy Protection Act)

- Regulates collection of *personal information* from children under 13 via online services (websites, advertising, mobile apps)
- Defines what data may not be collected or disclosed without verifiable parental consent
- Provides for how to seek verifiable consent from a parent before collecting any personal information
- Outlines responsibilities to protect children's privacy and safety online

COPPA and Remote Learning

EXAMPLE:

Online education modules produced by private sector partners who seek to collect personal information from children in order to market products/services

FERPA
Family Educational Rights and Privacy Act

Federal law that protects the privacy of student education records

Affords parents the right to:

- Access and inspect their child's education records
- seek to amend records, and
- exercise some control over the disclosure of records.

FERPA: Educational Records

Education Records include information about a student maintained in schools in any recorded way, such as handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. Examples:

- Date/place of birth, parent/guardian address/contact info;
- Grades, test scores, courses taken, academic specializations and activities, official letters regarding a student's status in school;
- Special education records;
- Disciplinary records;
- Medical and health records;
- Attendance, schools attended, courses taken, awards, degrees earned;
- Personal information (student ID, SSN, picture).

FERPA: Requirements & Restrictions

Consent is required for disclosure of records unless an exception applies.

- FERPA definition of PII is different from definition under state data breach laws.
  - Very broad (like new state privacy laws such as CCPA)
  - Student name, parent name, address, SSN, student ID no., DOB, mother's maiden name, "other information" that is linked or linkable to a particular student, etc.

FERPA: Logging and Disclosures Exceptions

Recordkeeping

Schools must keep log in the student's record of who has requested or obtained access to the student's record and the "specific legitimate interest" for obtaining access.

Available only to parents, the school official/assistants responsible for the custody of such records, and persons authorized by statute to conduct audits.

Does not apply to "exception" disclosures.

<u>Notice</u>

Annual Notification of FERPA rights

Directory Information

FERPA: Breaches

Breach Response Actions Required:

- Reporting incident to the Dept. of Ed./FSA
- Notation of student file/log that unauthorized access occurred

- No private right of action under FERPA
- Notice to students/parents is not required

State Data Breach Notification Laws

- All 50 states, D.C., and the territories have enacted breach notification laws
- Not uniform, though commonly require:

Typical Data Breach Notification Law

An entity that maintains computerized “personal information” or “personally identifiable information” must disclose a “security breach” to any state resident whose unencrypted, unredacted personal information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

Pennsylvania DBL

- “The unauthorized access **and** acquisition of *computerized* data that **materially compromises** the *security or confidentiality* of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.
- Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.”

What is “Personal Information?”

Name
+ another
sensitive
data element:

Personal Information - PA

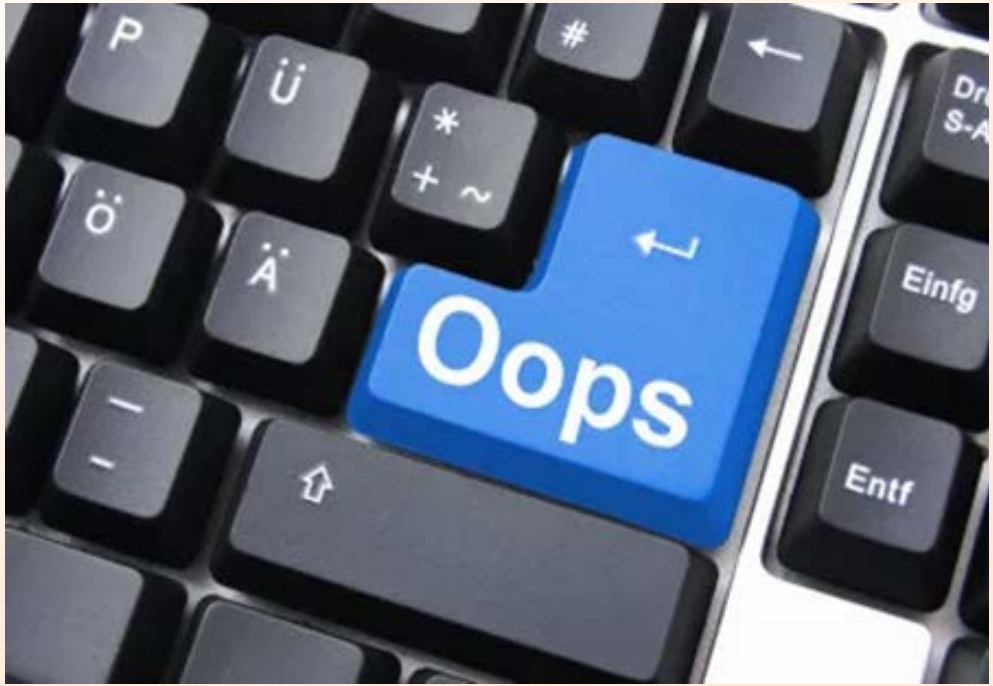
- “An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
  - Social Security number.
  - Driver's license number or a State identification card number issued in lieu of a driver's license.
  - Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
- Does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.”

Notice Requirements – PA

- “An entity that maintains, stores or manages computerized data that includes personal information **shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident** of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person… without unreasonable delay.”

Common Threats

- Business Email Compromise
  - Phishing
  - Social Engineering
  - Unsecure Email Platforms/Personal Accounts



Common Threats

- Ransomware
  - Evolution and sophistication
  - “Double extortion”
  - OFAC advisory
  - Colonial Pipeline

The Ransom Note

All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we **REALLY CAN** recover data - we offer you to decrypt samples.
You can contact us for further instructions through:
Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

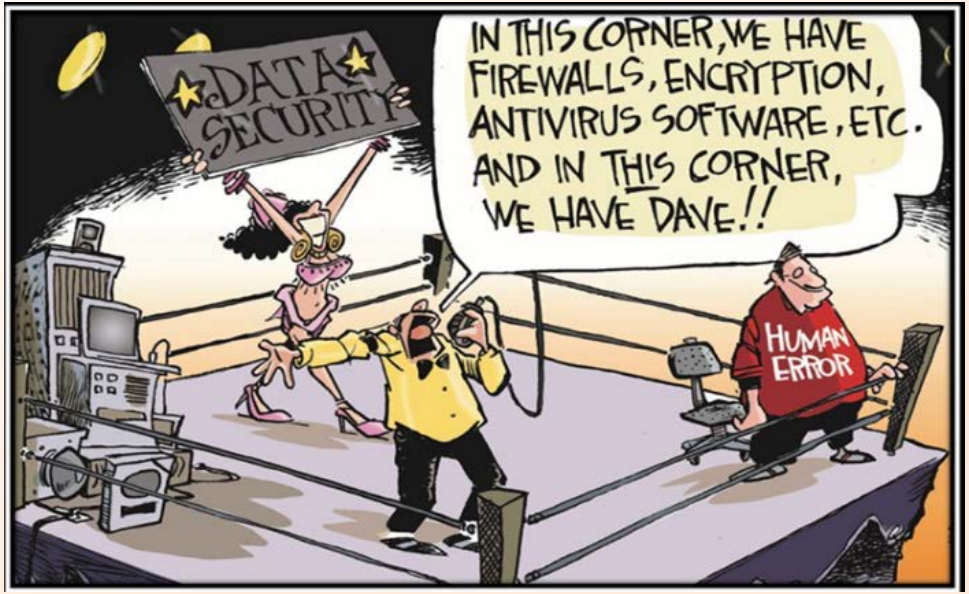
http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION:
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

Common Threats

- Human Error
  - Misdirected email



Notifications

- Any one of these “incidents” can, upon investigation, reveal a data “breach” that triggers notification or reporting obligations.
- Paying a ransom demand or asking for a return of the data does not necessarily dispose of the issue.
- An ounce of prevention (and preparation) is worth a pound of cure.

Private Claims For Breaches

Breach lawsuits, including class actions, are routinely filed around the country.

- Negligence
- Breach of contract
- Other theories

Defenses to Claims: Sovereign Immunity?

Does sovereign immunity protect schools against these claims?

Pennsylvania's Political Subdivision Tort Claims Act

EXCEPTIONS:

- Vehicle liability
- Care, custody or control of personal property
- Care, custody or control of real property
- Trees, traffic controls and street lighting
- Utility services facilities
- Streets
- Sidewalks
- Care, custody and control of animals

Other Defenses to Claims

- Liability Cap (if a tort claim): $500,000
- Article III Standing

    Injury is not sufficiently concrete or is speculative

Best Practices – Security & Privacy

- Review and re-assessment of policies and procedures
- Security Awareness Training
- Assembly of an Incident Response Team (IRT) and Disaster Recovery/Contingency Plans
- Vendor Agreements
- MFA
- Firewalls & AV
- Activity Log Monitoring
- Security Updates and “Patches”
- Viable and useful backups
- Risk Analyses
  - Vulnerability Scans
  - Penetration Testing

Questions?

Sandy B. Garfinkel
412.566.6868 | sgarfinkel@eckertseamans.com

Stephenie G. Anderson Scialabba
412.566.1925 | sscialabba@eckertseamans.com

ECKERT SEAMANS
ATTORNEYS AT LAW