Education Data Security

Understanding the Cyber Threat & Best Practices for Reducing Risk

Mike Tassey
PTAC Data Security Advisor

United States Department of Education
Student Privacy Policy Office
Privacy Technical Assistance Center

Who are we?

- PTAC is a technical assistance center under the Student Privacy Policy Office (SPPO)
- Provide guidance on FERPA, student privacy & data security
- Resources on our website: https://studentprivacy.ed.gov/
  - Trainings and Webinars
  - Documents
  - FAQs
- We are not the FERPA Police

FERPA & Data Security

Why doesn’t FERPA tell me **<u>how</u>** to protect student records?

FERPA & Data Security

While FERPA doesn’t specify security controls & technology requirements, it does require you to protect PII from student records:

- *From unauthorized disclosure*
- *To ensure that PII is only used for its intended purpose*
- *To ensure that PII is properly destroyed when no longer needed*

FERPA & Data Security

These requirements map well to commonly accepted IT Security Best Practices:

Technical Controls

Administrative Controls

Physical Controls

FERPA & Data Security

While FERPA may not explicitly require it, smart organizations will employ a diverse set of security & privacy controls that help them protect student records!

Security Controls

- Best Practices
- Commensurate with data sensitivity

Policy & Mgmt.

- Strong governance and policy
- Good Metrics & Risk Analysis

Data Security - Why

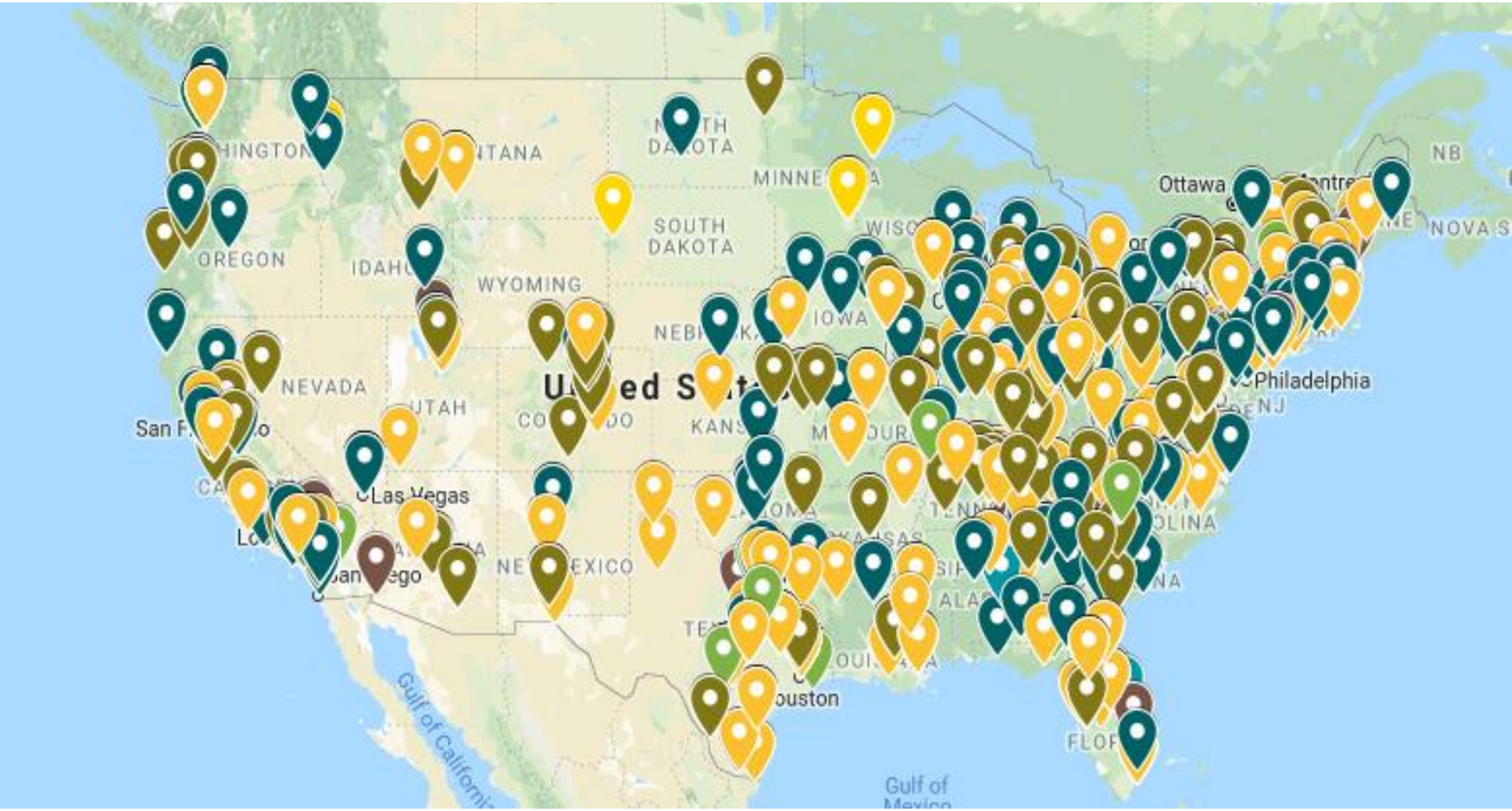
- FERPA requires it.
- Students deserve it.
- More data in more places
- Cybercriminals developed a taste for schools

We collect more, move more, use more & lose more data than ever before.

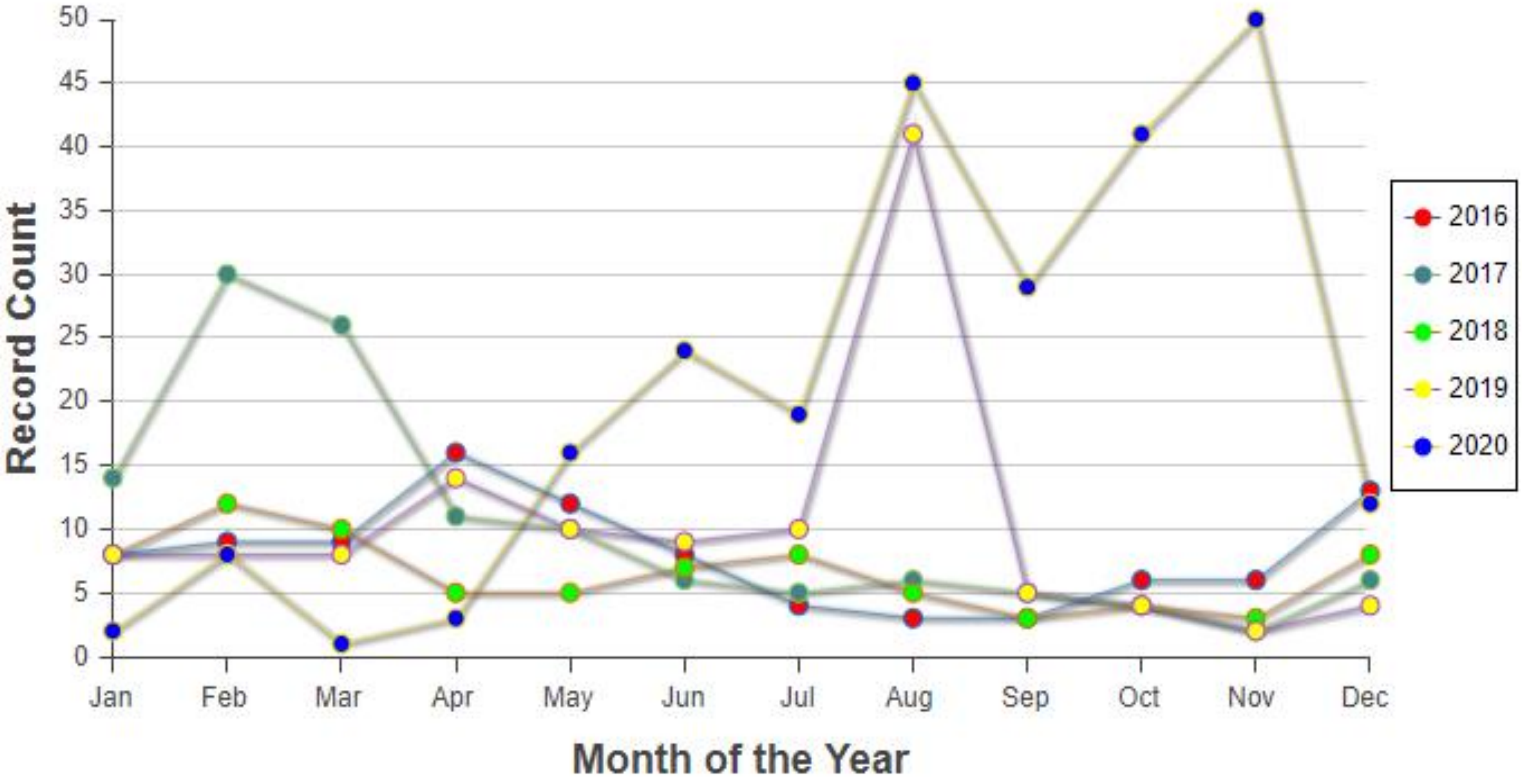
Problems in Education Data Systems

- Lack of training / Awareness
- Remote learning tools
- Third Party Applications & Service Providers
- Cloud platform insecurity / misconfiguration
- The Internet of Things (IoT)
- BYOD / Working from home
- Legacy & Unpatched Software / Hardware

Data Breaches in Education

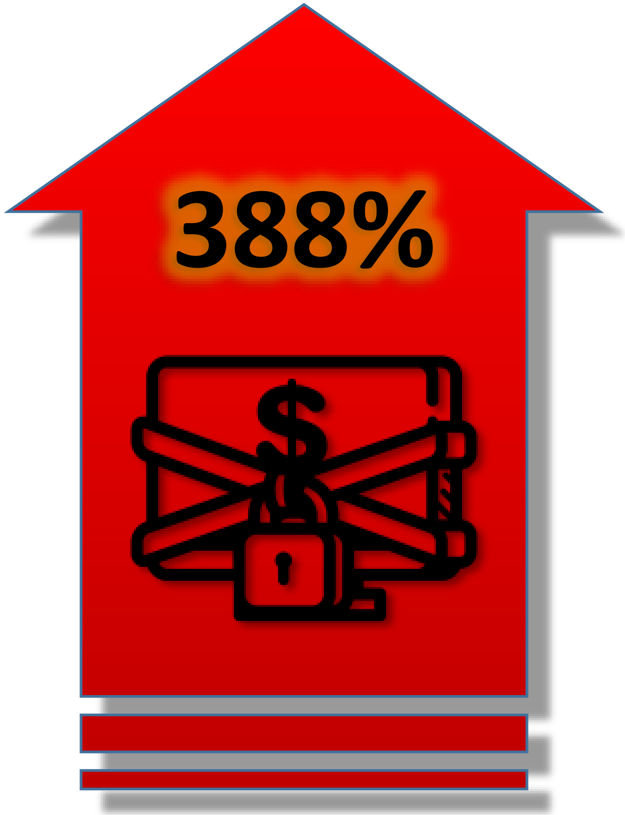


Data Breaches in Education



Ransomware in Schools

- Ransomware attacks increased 388% in the third quarter of 2020
- THE biggest threat to education data right now
- New attack strategies mean increased impact & reduced options for victims
- Bad actors are targeting education specifically



But I don’t work in IT?

- **Many breaches start with social engineering**
- **Attackers target people, not the technology first**
- **Use stolen credentials once inside**

Ransomware in Schools

The best time to attack is "Back to School" time

- Staff Ops Tempo is very high
- New systems and technology
- "Rusty" staff returning to work after a long break
- High activity level offers obfuscation for attackers
- Data breaches at the beginning of the school year are more likely to result in payoff

How Can You Increase Security?

- Leadership must create a “Culture of Security”
- Engage staff and students with training
- Create incentives & break down barriers
- Focus on resilience and readiness
- Establish an organizational standards
- Remove roadblocks that result in work-arounds

How Can You Increase Security?

DOCUMENTED, REPEATABLE PROCESSES DRIVEN BY SOLID ORGANIZATIONAL POLICY

METRICS

Perform Annual Risk Assessments

"The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact."

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

Formal organizational process involving leadership, IT, and organizational stakeholders

Four stages:

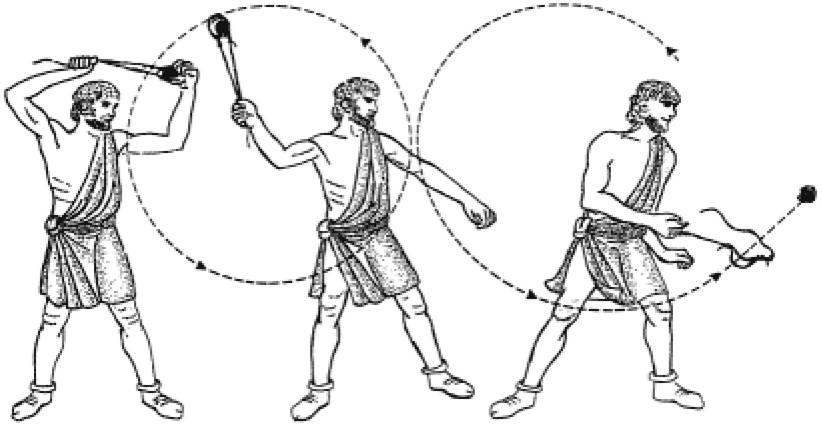
- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis –** *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation –** *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control –** identifying and applying mitigating controls to reduce the risk based on analysis

Develop Incident Response Plans

- Identify a PoC responsible for security
- Understand the legal requirements around IR and data breach
- Create comprehensive IR plans and policies
- Not just IT… Include all stakeholders
- Build strong communications and messaging platforms
- TEST YOUR PLAN!!!

The Reality is

Attackers only have to get lucky once…



Top Tips for Reducing Risk

- Train users effectively
- Identify & catalog internet facing devices and software
- Update software/firmware regularly
- Incorporate IoT devices in IT processes
- Carefully vet applications & service providers
- Plan for the worst!

Contact information

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

https://studentprivacy.ed.gov

(855) 249-3073