Vendor Considerations for IT Security

A4L Conference

Ross Lemke
Director
Privacy Technical Assistance Center (PTAC)

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

Disclaimer

This content was produced by the U.S. Department of Education's Student Privacy Policy Office (SPPO) through its Privacy Technical Assistance Center (PTAC) for the purposes of this presentation. This presentation is provided for informational purposes only. Nothing in this presentation constitutes official policy or guidance from the U.S. Department of Education.

Official policy and guidance can be found on our website at https://studentprivacy.ed.gov/.

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

SPPO/PTAC Resources

Visit our Website https://studentprivacy.ed.gov/ for great resources like

- *Online Training Modules*
  - FERPA 101
  - FERPA 201
- *Guidance Videos*
  - Email and Student Privacy
  - Communicating with Parents about Data Use and Security
- *Resource Documents*
  - Data Security & Data Breach Checklists
  - Incident Response Exercise Training Kits
- *Recorded Webinars*

Subscribe to our Newsletter!

The U.S. Department of Education is releasing new material all the time.

To stay abreast of these developments, please join our Student Privacy Newsletter: https://studentprivacy.ed.gov/subscribe-student-privacy-newsletter

What's This All About?

The student data ecosystem is a BIG place, and it's getting bigger every day!! But there is a lot of misunderstanding about who is responsible for what when we talk about schools and vendors. Today is about shining some light on that!

Cybersecurity is not an ***us*** problem or a ***them*** problem… it is a "we problem."

Let's Start With FERPA

What is FERPA?

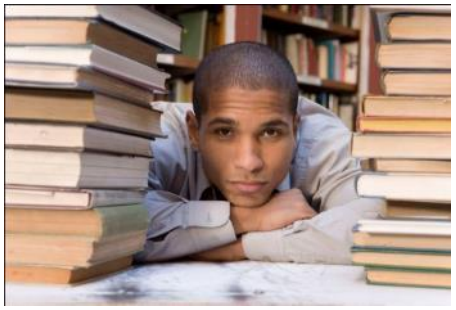
A federal privacy law that affords parents the right to:

- have access to their children's education records,
- seek to have the records amended, and
- consent to the disclosure of personally identifiable information from education records, except as provided by law.

To Whom Does FERPA Apply?

Elementary

Secondary



Postsecondary

U.S. Department of Education Funding

But What About Vendors?

- FERPA doesn't apply to vendors… *but don't think you are off the hook*
- EdTech vendors most often act *"on behalf"* of the school
- By extension, this means that FERPA rules still apply to the data, and to your customers!

FERPA Pop Quiz!

1. FERPA does **not** require you to use specific technology to protect IT data systems?

   (T) F

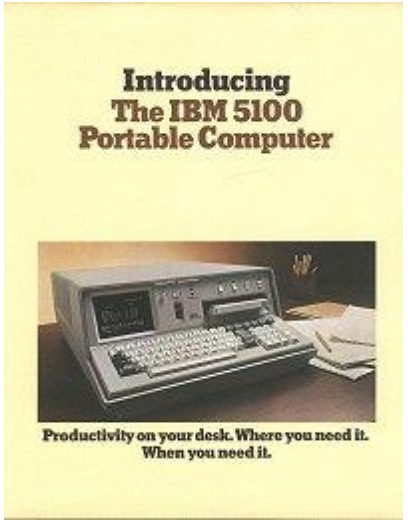
2. All FERPA violations are Data Breaches.

   T (F)

FERPA & Data Security

Why doesn't FERPA tell me **how** to protect student records in my data systems?

The world has changed



When FERPA was passed in 1974:

- Average house price was $38k
- Average income was $11k
- Federal spending was “only” $269B
- You could buy a PC for the low, low price of $20k

And…

- Disco was still cool
- Education records were mostly papers in the principal’s office

FERPA & Data Security

While FERPA doesn't specify what security controls & technology, it does require you to protect PII from student records from disclosure and to:

- *Ensure that school officials obtain access to only those education records in which they have legitimate educational interests*
- *Identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses PII from education records*
- *Ensure to the greatest extent practicable that any entity or individual designated as its authorized representative uses, protects, and maintains / destroys data in accordance with FERPA requirements*

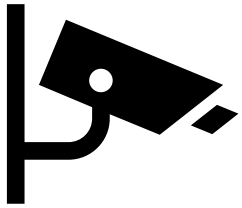
14

FERPA & Data Security

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

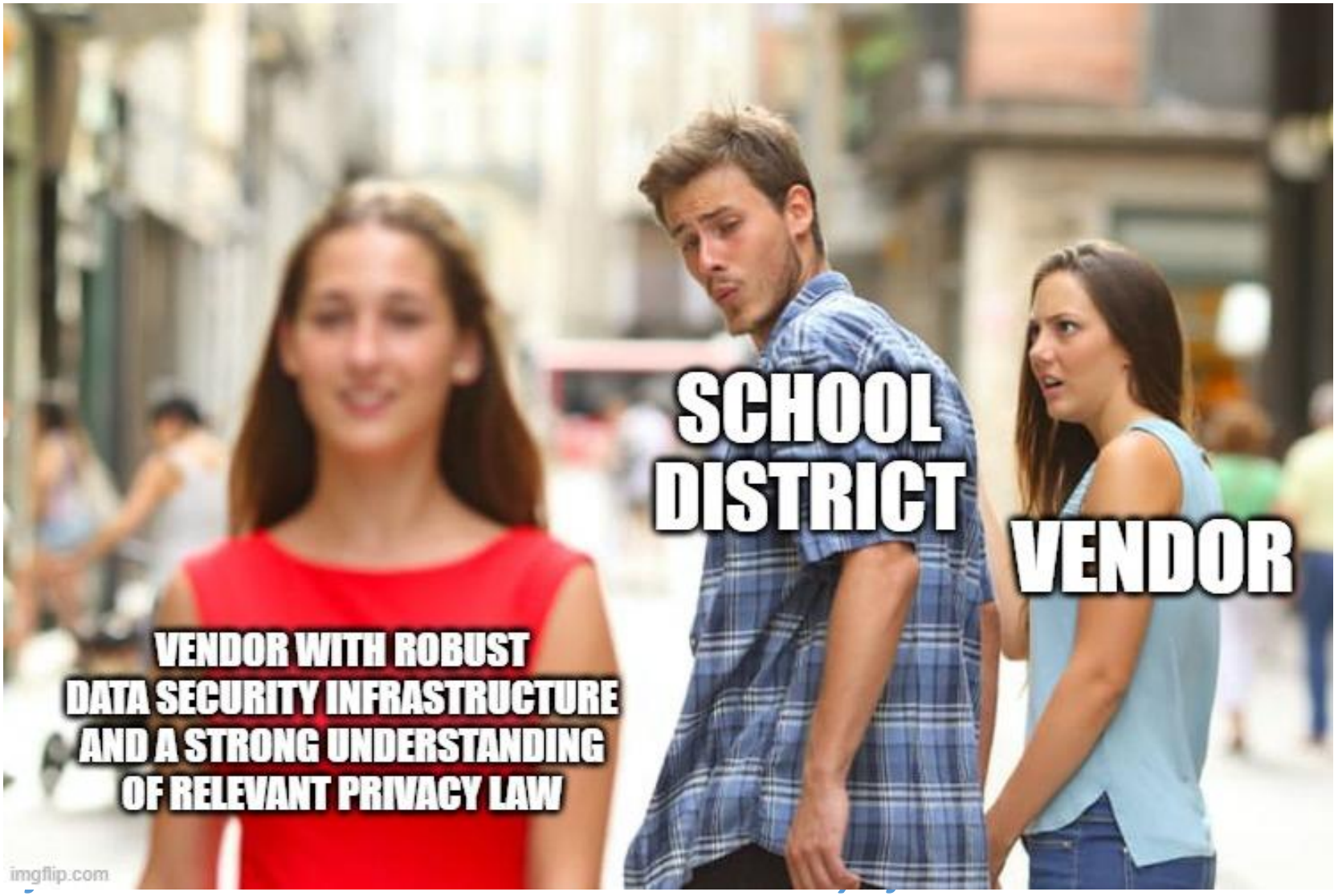
Technical Controls

Administrative Controls



Physical Controls

15


SCHOOL DISTRICT
VENDOR
VENDOR WITH ROBUST DATA SECURITY INFRASTRUCTURE AND A STRONG UNDERSTANDING OF RELEVANT PRIVACY LAW
imgflip.com

So, What Do We Mean By Vendors?

- Student Information Systems (SIS) platforms & software
- Office automation & productivity apps
- Educational apps
- Core business services and functions
- Online Educational Services

What are the Challenges?

- Schools are increasingly contracting out school functions
- New types of data, new methods of storing, processing and leveraging these data.
- Non-traditional business models, click-wrap, no 2-party written contract, etc.
- Commercialization, harvesting, meta-data, and marketing
- Enabling vendor business models to work while still protecting student privacy and FERPA compliance

The Rules Change Depending on "How" You Get the Data

- FERPA has a "general consent rule"
- Schools either have to obtain consent or the data falls within an "exception" to the consent rule
- EdTech vendors typically obtain records under one of two main exceptions:
  - ***Directory Information***
  - ***School Officials***

Directory Information Exception

Allows schools to release certain non-critical information without consent. A few examples:

- *Name, address, telephone listing, electronic mail address*
- *Date and place of birth*
- *Photographs*
- *Weight and height of athletes*
- *Degrees & awards received*

This is commonly used for yearbooks, directories, concert programs, etc.

Directory Information Exception

This information is not often used with EdTech

Remember:

- *Parents can opt-out, so you may not get all the data*
- *The school can still restrict your use of the data via written agreements / contracts*

School Official Exception

Schools or LEAs can use the School Official exception to disclose education records to a third-party provider (TPP) if the TPP:

- Performs a service/function for the school for which it would otherwise use its own employees
- Is under the direct control of the school/district with regard to the use/maintenance of the education records
- Uses education data in a manner consistent with the definition of the "school official with a legitimate educational interest," specified in the school/LEA's annual notification of rights under FERPA
- Does not re-disclose or use education data for unauthorized purposes

Okay, What About Metadata?

Metadata that have been stripped of <u>all direct and indirect identifiers</u> are not protected under FERPA. *(NOTE: School name and other geographic information can be indirect identifiers in student data.)*

Properly de-identified metadata may be used by providers for other purposes *(unless prohibited by other laws or by their agreement with the school/district).*

Best Practices for Protecting Yourself & Your School Customers

- **Maintain awareness of other relevant laws**
- Be aware of what data the school provides and how it is being used and maintained
- Have policies and procedures to evaluate your IT security controls against school expectations and FERPA requirements
- When possible, use a written contract or legal agreement
- Be transparent & open with schools about your data security / privacy processes

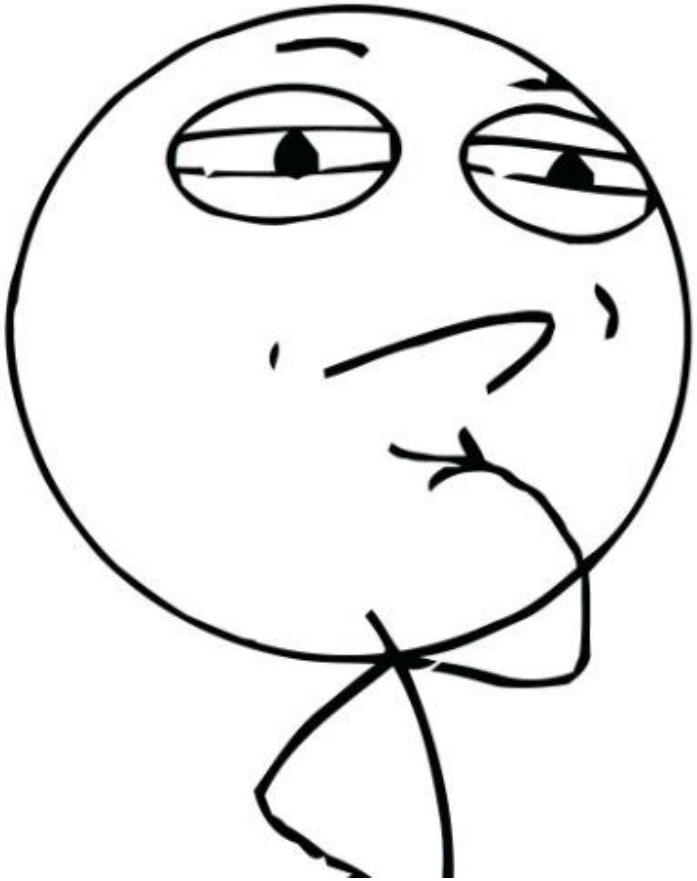
Best Practice Contract Provisions for EdTech Apps & Services

- Security and data stewardship provisions
- Data collection provisions
- Data use, retention, disclosure, and destruction provisions
- Data access provisions
- Modification, duration, and termination provisions
- Indemnification and warranty provisions

Red Flags in Your ToS?

- Limited definitions of protected data
- Narrow definitions of what constitutes de-identified data
- Data re-use, sale, or marketing to education users *(such as parents or students)*
- Modification of ToS without notification
- Lack of data collection limits, collection of unneeded data
- Clauses containing "Without notice"
- Data redisclosure to third-parties without notice
- Any provision that grants a "license" to use or retain data or content for any purpose
- Any limitation of the school to access or control of its own data

So, What About IT Security?



Schools are Struggling

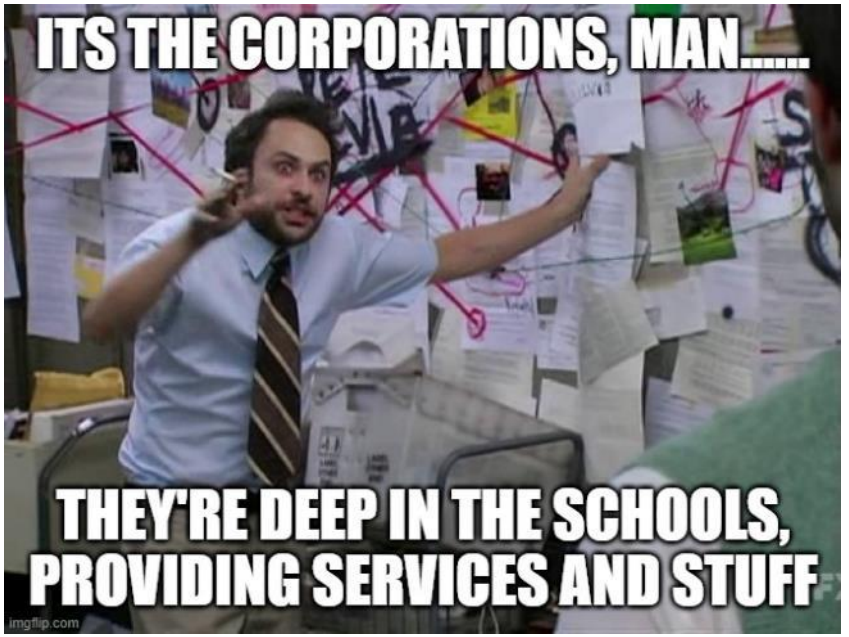
≠

Cyber budget = $15 Billion

Cyber Budget = Gym Teacher

Why are we talking about this

- Schools can't possibly build the infrastructure and architecture they need
- Vendors provide awesome capabilities at an economy of scale
- Vendors occupy this incredibly important niche but often don't understand the "why"
- Schools are not the same as other industry sectors or customers



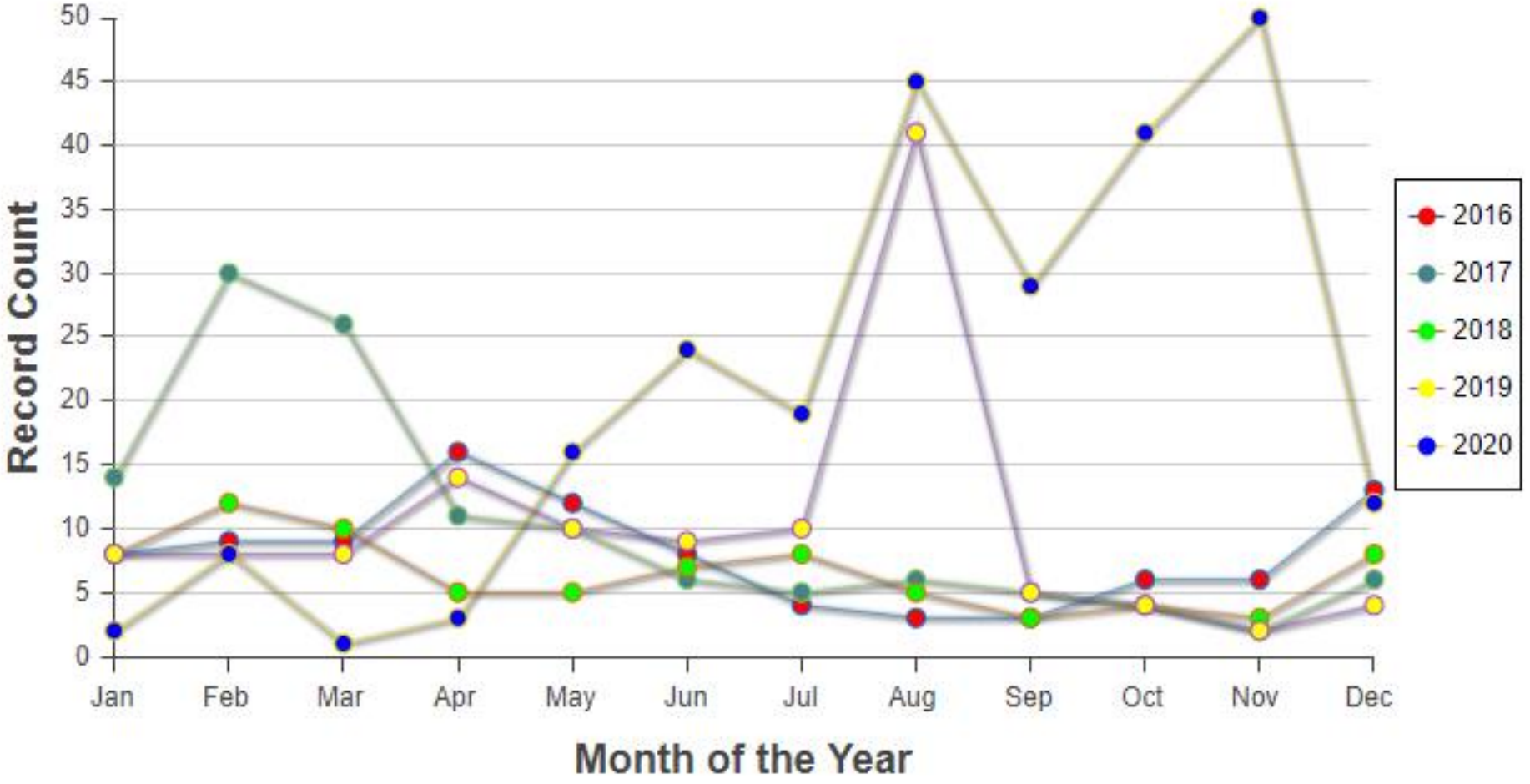
So, What's the Rub?

- If **one school** has a security incident, that's bad
- If **one vendor** has a security incident… *That's national news!*

Cyber-Security in the Education Space

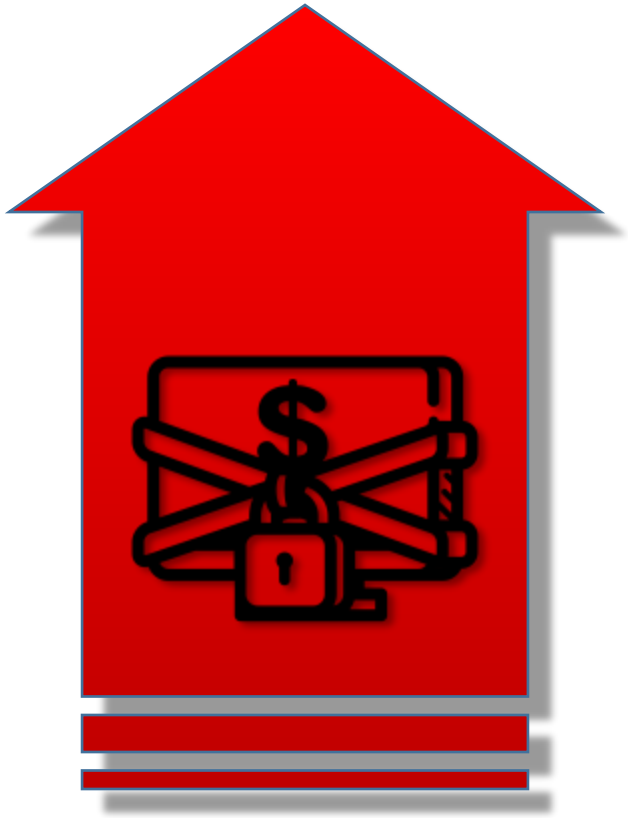
You want to see a dead body?

Data Breaches in Education



Ransomware in Schools

- Ransomware attacks increased massively 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

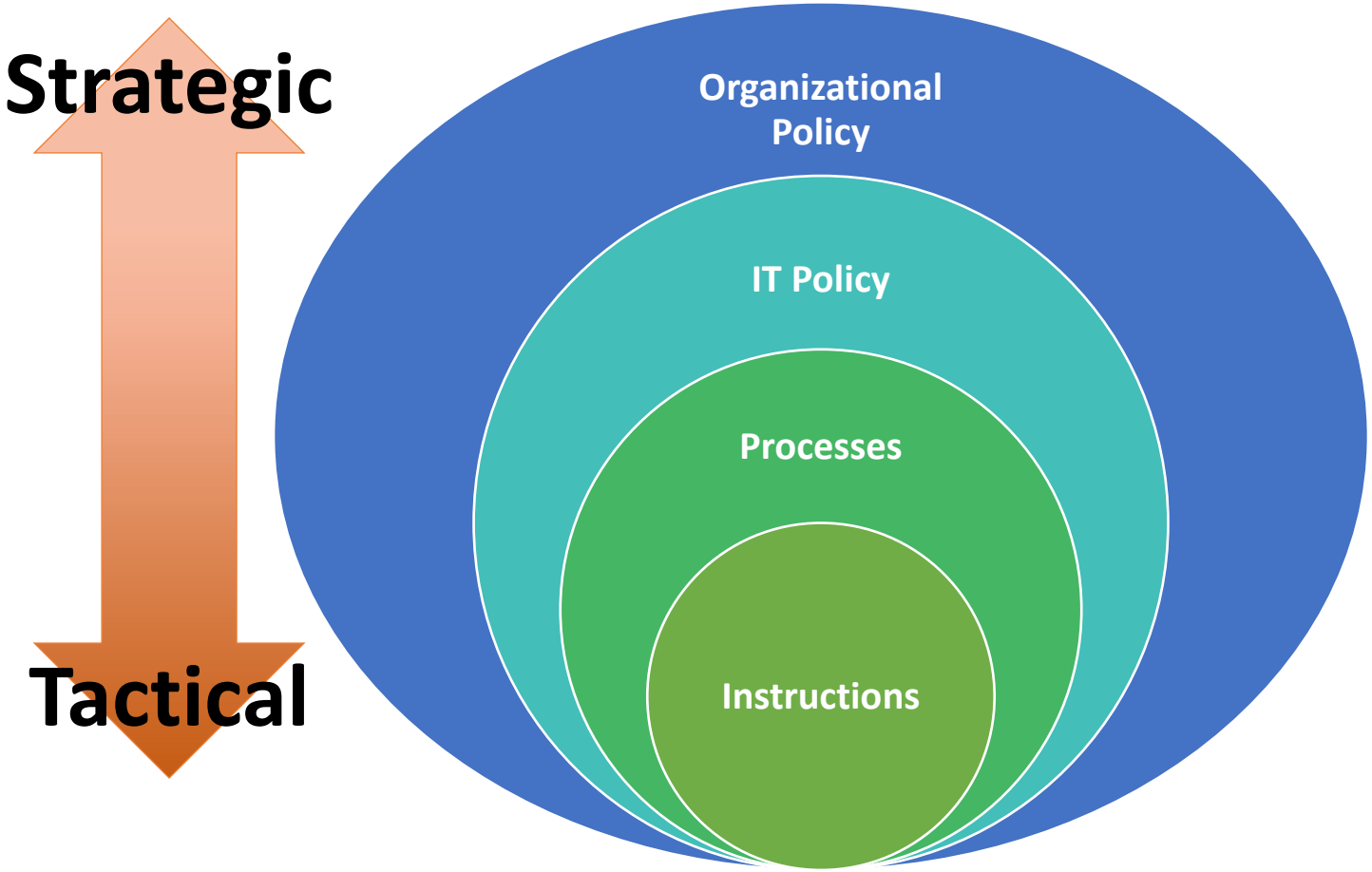


How to Operationalize Security?

DOCUMENTED, REPEATABLE PROCESSES DRIVEN BY SOLID ORGANIZATIONAL POLICY

METRICS

(Groan) Start With Policy



These are the Basics

- Privacy & IT security Training annually
- Vulnerability Management
- Control Board / Risk Management Board
- Incident Response
- Account Management
- Data & System Standards
- Enforcement

Privacy & IT Security Training

- **Annual threat awareness training for all employees, faculty, administrators**
- **Focusing on cyber-hygiene, social engineering awareness, and threat**
- **Great time to revisit AUP and employee expectations for security**

Vulnerability Management

- Build organizational policies and processes to identify and mitigate vulnerabilities
- Create a Patch and Vulnerability Group responsible for centrally managing vulnerability mitigation efforts
- Starts with good asset inventory data, automated tools, risk classification
- Track & coordinate remediation according to organizational standards set in policy

Formalized Risk Management

- Manage risk at a strategic level, not tactical
- Organizational risk is often wider than a single system or business unit
- Create a formalized body to consider all kinds of risk (physical, digital, etc.) to accept or mitigate risk, and set acceptable risk thresholds
- Manage system changes through this body to ensure that data risk is continually managed as the system grows or changes

Incident Response is a MUST

An Incident Response Team is a team of individuals tasked with preparing for and responding and mitigating an emergency. This could be any type of emergency from natural disasters to cyber-attacks and data breaches.

Incident Response Teams are often comprised of several core members and bring in others as needed depending on the nature of the incident:

- Executive Leadership
- Legal Counsel
- Communications
- IT
- External Partners
- Departmental Leadership
- Facilities

Standards Are Your Friends

Reliable data security programs all have one thing in common… control:

- *Create standard software loads & enforce them*
- *Same applies to Boundary Control (fw rules)*
- *Police for compliance*

Process changes through CCB or similar process

Enforcement

- Have users read and sign Acceptable Use Policies annually after training
- Leverage automated tools to check for system configuration and software standards compliance
- Make it easy for users to ask questions and get solutions rather than workarounds
- Advertise data security expectations and sanctions for non-compliance

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

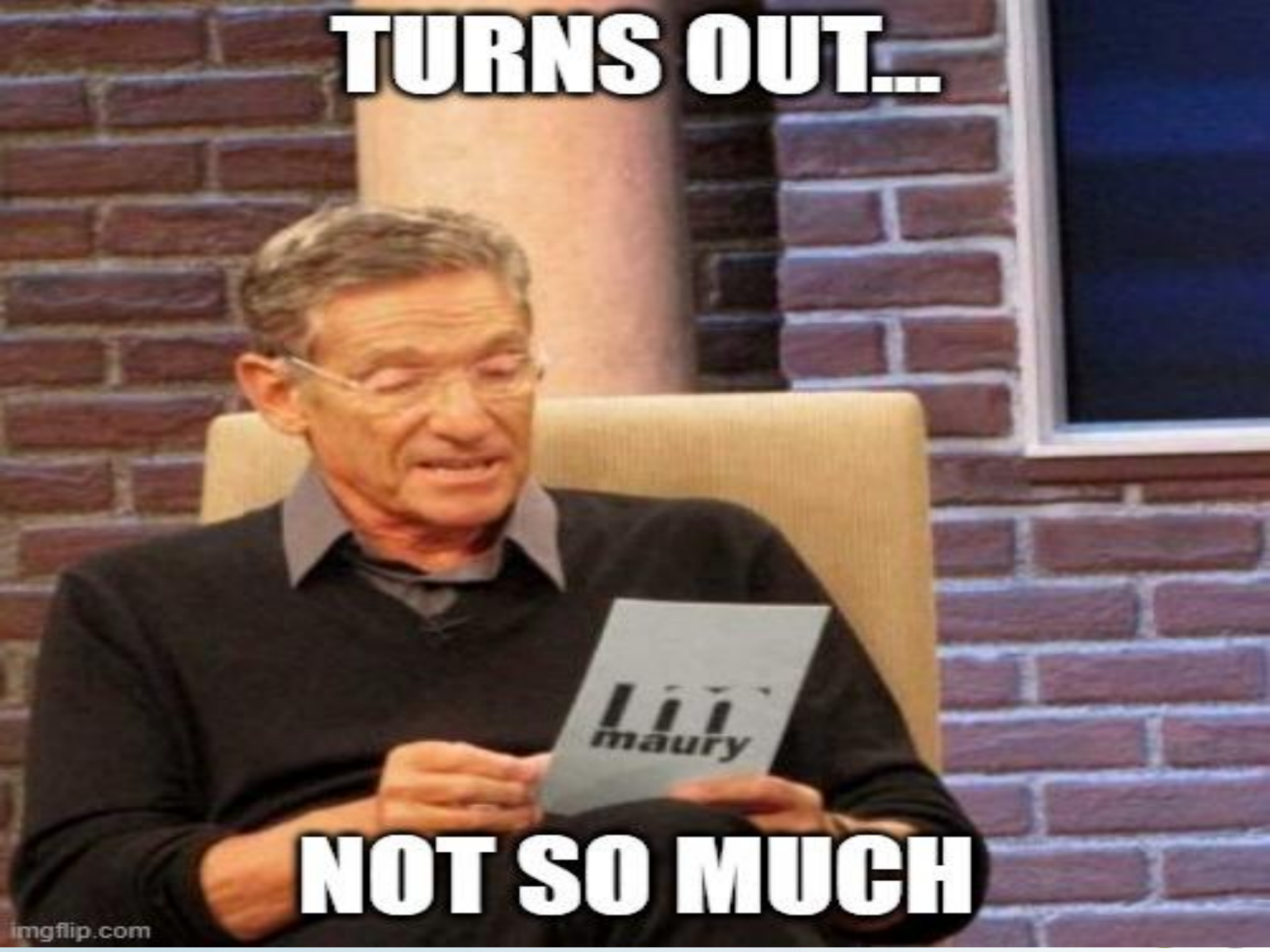
Four stages:

- **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

Where Does the Data Live

So, by now you are thinking, “Duh, we’re an IT company… of course we know this stuff”.

- Misconfigured AWS S3 buckets
- More than 100k students and their own source code / digital keys
- More than 117 million files and 22TB of data
- Student names, emails, performance reports, grades


TURNS OUT...
maury
NOT SO MUCH
imgflip.com

Where Does the Data Live

- Because vendors are a consolidation point for MANY schools, any weakness is a critical one
- One unconfigured S3 bucket, even from years ago can be devastating
- Where else does the data exist?
  - *Your partners? What about their security?*
  - *Shared datacenters / cloud services*
  - *Think about how data flows through these interconnected systems*

Be able to articulate how you provide a higher level of assurance.

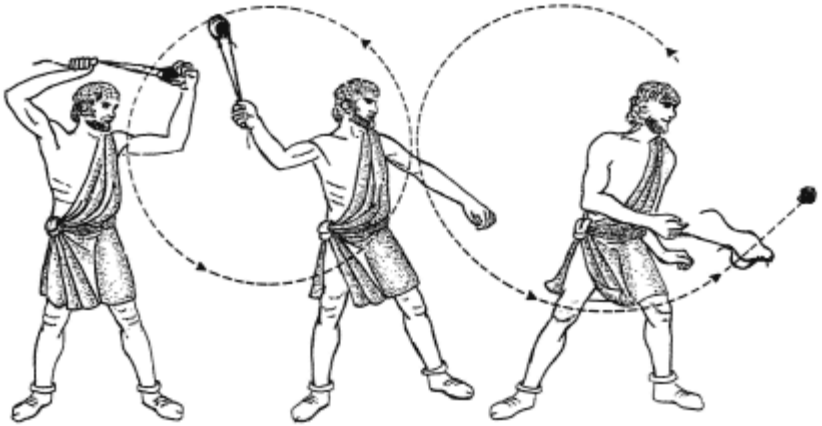
What Happens @ The End?

One area vendors often forget about is what happens when the client is no longer a client?

- FERPA data is not yours to keep
- What data might remain? Do you purge the data somehow?
- What about FERPA data that may be present in backups?
- Think about the whole data lifecycle:
  - Can the school REALLY delete data?
  - Can YOU really delete the data?
  - How long until it is gone and using what methods?

The Reality is

Attackers only have to get lucky once…



CONTACT INFORMATION

United States Department of Education,
Student Privacy Policy Office (SPPO)

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

privacyTA@ed.gov

https://studentprivacy.ed.gov

(855) 249-3073