Data Breach Apocalypse:
Incident Response When It Is Not Your Fault

03/19/2025

Ross Lemke
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.

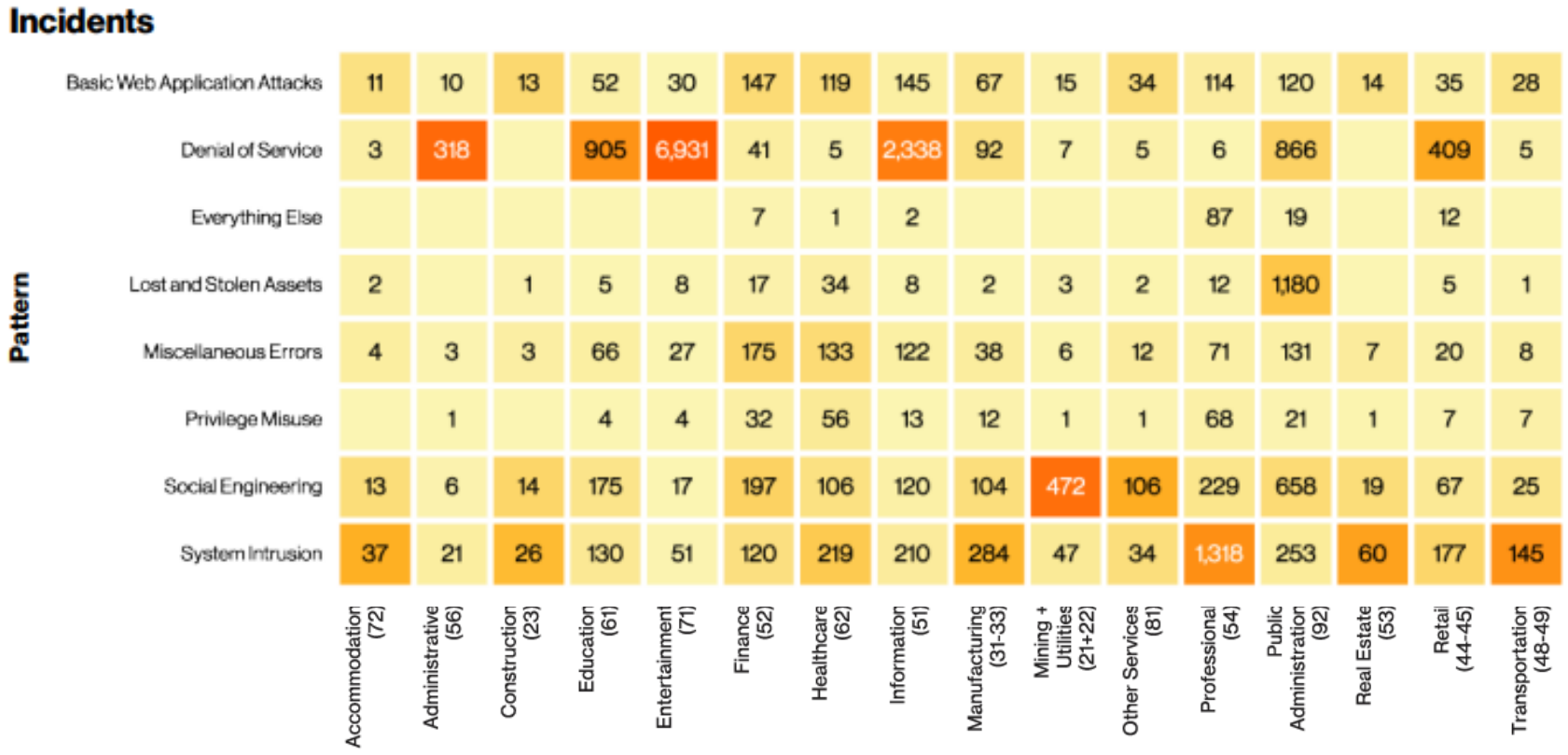
To stay abreast of these developments, please join our Student Privacy Newsletter: https://studentprivacy.ed.gov/subscribe-student-privacy-newsletter

Data Breaches Happen

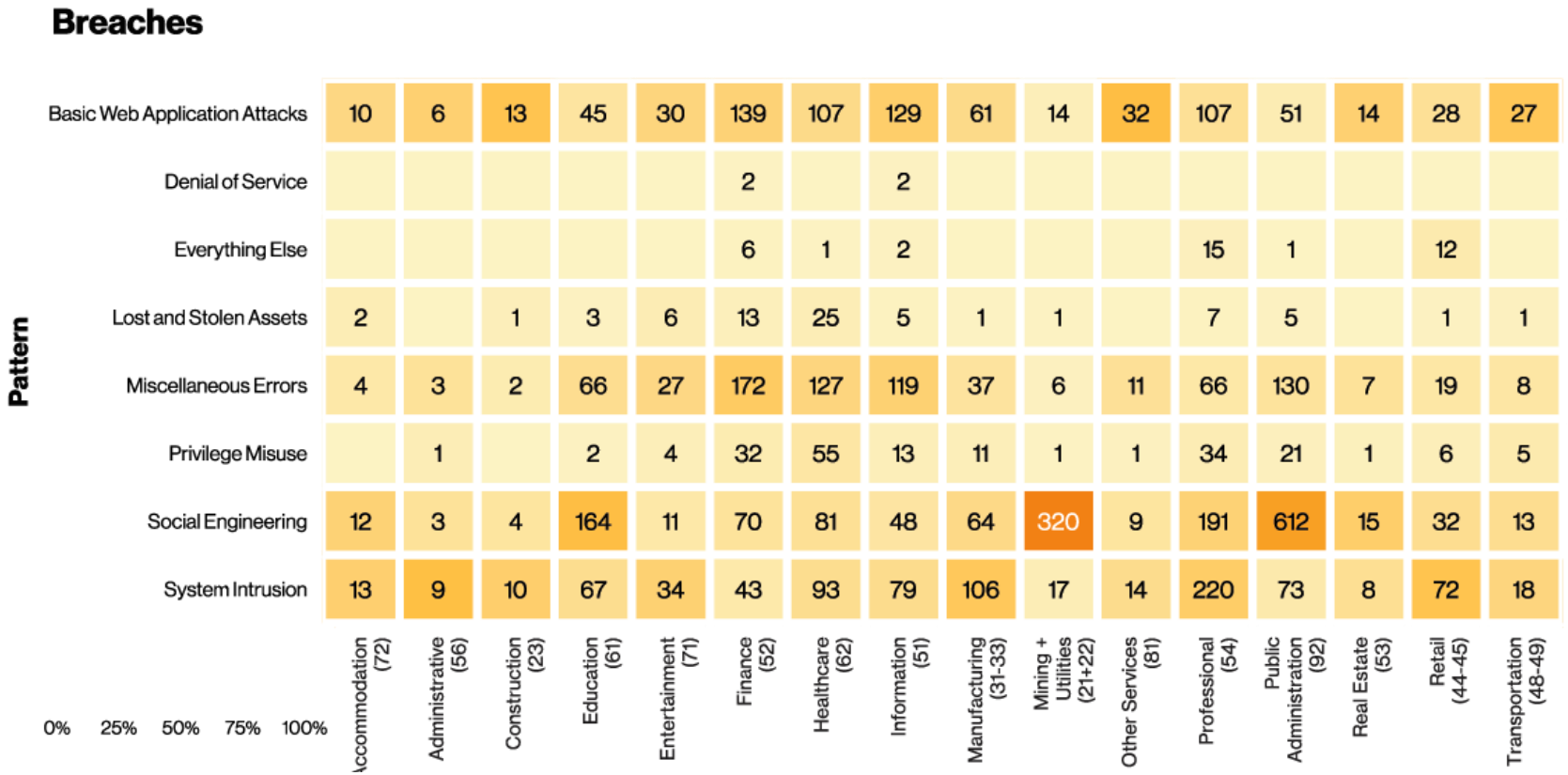
In the Recent Past

- More than 3000 schools impacted by data breaches
- Thousands of “other” incidents
- Dozens of large breaches involving thousands of victims
- School closures in major cities
- Billions of dollars in costs for remediation

Digging Deeper



Digging Deeper

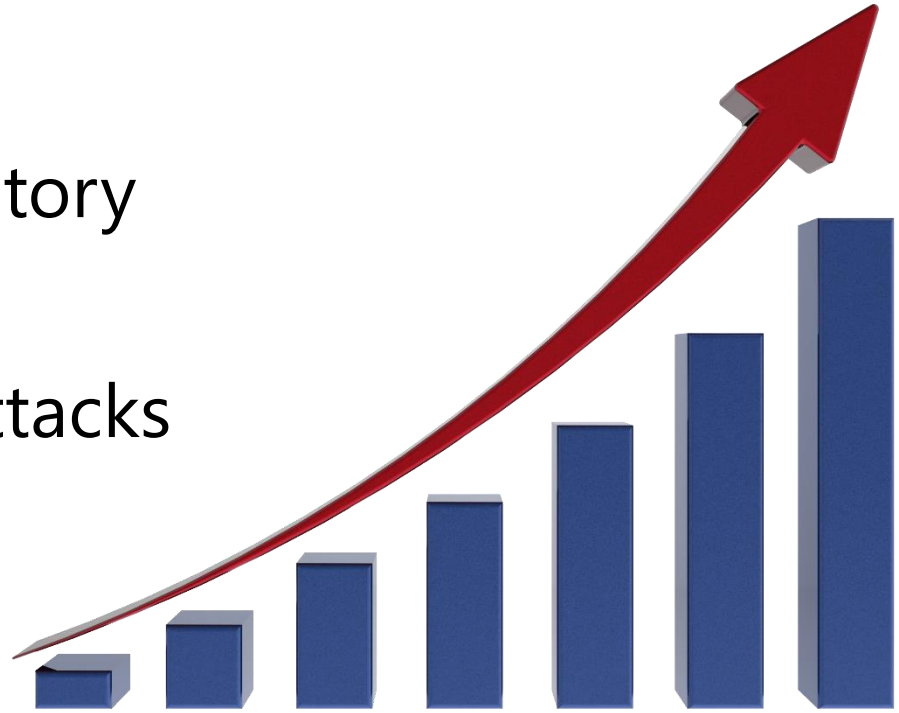


The Bottom Line

- Education == Retail and Finance
- **Employees** and **Staff** are going to be the way in
- If it isn't Ransomware, its going to be DDoS
- You need to spend **Time** and **Resources** on **training**
- IR Plans and process better be tailored to meet these threats

Data Breach Impacts to Education

- Billions of dollars in costs
- Downtime from days to weeks
- Legal liabilities & regulatory penalties
- Further targeting and attacks
- Reputational harm



Preparing for a Cyber Incident

Outsourcing the Service Doesn't Outsource the Risk!

Schools outsource many of their functions to third-party vendors & service providers. Especially with big vendors, they think they are outsourcing their risk as well.

Remember, Even if the breach isn't directly within your systems, it's still your data.

Remember the Basics

- Have a Plan & Team
- Train your people
- Risk Assessments & Risk Management
- Annual IR exercises
- FERPA Compliance *(like written agreements)*

Understanding 3rd Party Risk

Data breaches in partner/vendor systems impact your students' data security.

Vendors value security, and many offer great protections, but do you know what they are?

Regardless of the type of service or vendor you contract with, there is a shared responsibility model there. You need to understand who is responsible for what!

Understanding 3rd Party Risk

Risk Factors for Vendors & Service Providers

1. May not enforce security best practices like encryption or audits
2. Insufficient data segregation/client separation
3. Inconsistent or ambiguous data usage & retention policies
4. Poor access controls, lack of MFA or SSO integration
5. Lack of ability for client oversight/audit or the promulgation of periodic 3rd party audits for assurance
6. Poor business continuity or disaster recovery processes

Names Don’t Matter

Just because you are working with a big-name vendor, doesn’t mean there is no risk. Evaluate your partners, demand accountability and responsiveness.

In the end, it’s YOUR school who will be in the newspaper.

Vendors & FERPA

Your vendors & service providers are generally going to be school officials, which means among other things that:

- ***They must perform a function the school would have done for itself***
- ***The school maintains "direct control"***
- ***The vendor only uses the student data for specified purposes and prohibits the redisclosure of the data***

In many cases, schools lack direct control but are still accountable

Incident Response & 3rd Parties

Successful response is all about planning. Do You:

1. *Have a breach notification clause?*
2. *Include your providers in IR activities?*
3. *Know your POC/who to call?*

Incident Response & 3rd Parties

Communications Strategies

Managing Public Perception & Parent Concerns

- Early, factual, non-speculative information
- Consistent messaging that focuses on actions taken and next steps
- Avoiding jargon, spin, or obfuscation

Incident Response & 3rd Parties

- When you are notified of the incident, reach out to your point of contact at the vendor
- <u>You need to know a few things:</u>
  - What happened?
  - What is impacted?
  - What are the next steps?
- Communication is PARAMOUNT!!!

What About Researchers?

Researchers are typically engaged to perform studies to improve education, not to deliver day-to-day services or manage operational data.

This means that they are most likely not acting as school officials, but under other exceptions, such as the studies exception or the audit/evaluations exception that have their own stipulations on data access, use, and disclosure under FERPA.

What is Different About Researchers?

Researchers are unlikely to be targeted individually by cyber-attackers, a breach involving researchers is more likely to be the result of improper handling or inadvertent disclosure.

If you work with researchers:

- *Have a strong written agreement*
- *Employ data minimization*
- *Bind individuals to data protection*

Let's Talk IR Secret Sauce

Secrets to *less Painful Incident Response:

- Not Owned by IT
- **Includes Legal Counsel & Public Affairs**
- Starts with Validation
- Continuous review & testing
- Incorporates lessons learned

Connect Your Team to Theirs

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*
- *Vendors*
- *Contractors*
- *Facilities*

Think of your partners, vendors, and service providers as FERPA views them.. Extensions of your own staff. Your Incident Response Team needs an incident point of contact there to connect the teams, working with them before an incident establishes those links.

Leadership Needs Information

- Your leadership needs information to mitigate harm, inform the parents, and manage organizational priorities
- 3rd party breaches are less about the actions and more about the information flow
- Inquiries need to prioritize key facts for decision makers
- Incident managers need to work closely with communications personnel to craft appropriate messaging

Legal Eagles

Legal Counsel is a huge benefit in incident response. This could be your local counsel, outside counsel *(or even cyber-insurance company).*

- Often confusing legal requirements
- Need to protect organizational interests
- Interfacing with 3rd party legal & insurance companies

Communications is KEY

Your Communications Pro's are the lifeblood of any 3rd party breach. You will not be overly burdened with information, which makes it important that you make the most out of what you have.

- Need concise, clear, consistent messaging both internally and externally
- Address the "unknown" by explaining what is happening and why
- Consistency of messaging conveys reassurance that the response is under control, even if much is not known

Include 3rd Parties in Exercises

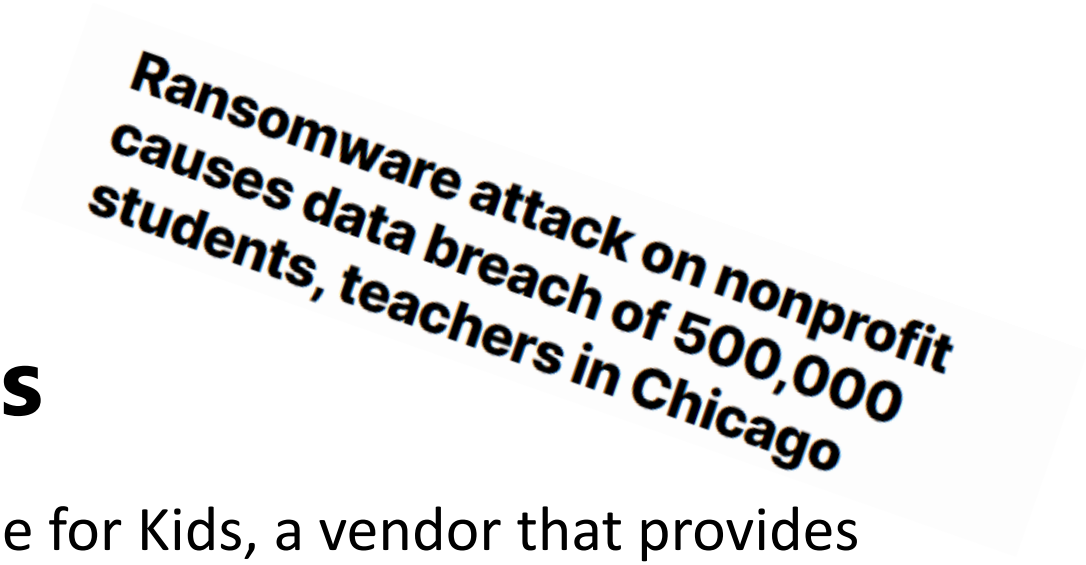
Do an Incident Response Exercise and invite all the right guests!

Response Exercises work out bugs and build competence

- *Why would you leave your partners & providers out?*
- *To the degree they are willing, include them in the planning phase, you might find some efficiencies*
- *A little work up front is worth hours or days of waiting for information from a vendor*

Let's Talk Over Some Examples

Example #1

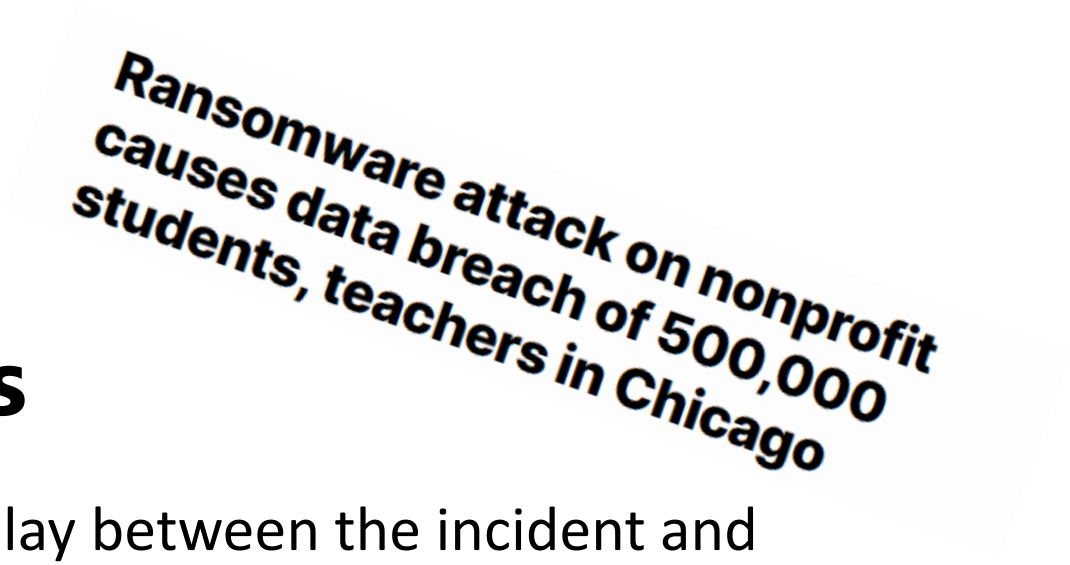


Battelle for Kids

In December 2021, Battelle for Kids, a vendor that provides educational services, was hit by a ransomware attack. The breach affected the data of approximately 495,000 Chicago Public Schools students and 56,000 employees

Exposed information included student names, dates of birth, schools attended, and employee identification numbers. Sensitive financial data and Social Security numbers were reportedly not affected

Example #1



Battelle for Kids

There was a five-month delay between the incident and notification hindered CPS's ability to respond promptly and take protective actions for affected students and staff. The lack of transparency from the vendor meant that CPS was faced with increased distrust among its stakeholders, parents, and community.

Example #1 – What can we take away

- Here again we see where it is important to have active connections with your vendors & partners
- Schools should proactively pursue information from any 3rd party suspected of having a breach
- Lack of partner transparency can have negative impacts on YOUR organization in the eyes of your constituents
- This incident showed the importance of contract requirements specifically in timely breach notification and data encryption practices.

Example #2

Snowflake

In 2023, Los Angeles Unified School District experienced a significant data exposure due to a breach involving their third-party data storage vendor, Snowflake. Attackers gained unauthorized access to sensitive information held within Snowflake's systems exposing extensive personal information, including student records, teacher data, and administrative details. Hackers reportedly obtained **millions of records** and attempted to sell the data online

Example #2

Snowflake

In 2023, Los Angeles Unified School District experienced a significant data exposure due to a breach involving their third-party data storage vendor, Snowflake.

The attackers took advantage of weak authentication practices and poor credential hygiene to steal credentials for the platform and used these stolen credentials to infiltrate Snowflake accounts and download sensitive data, which they later attempted to sell on cybercrime forums. LAUSD data for sale included student names, addresses, grades, and other sensitive records.

Example #2 – What can we take away

- Vendors should implement robust access controls and data/client segmentation, limiting the scope of data available to any single-entry point
- Schools should reassess how they approach contracts with third-party vendors, ensuring agreements included strict security obligations, regular audits, and clear notification timelines in the event of a breach
- Comprehensive data encryption both at rest and in transit is a must to reduce the risk of exposure during a breach.

Example #3

Aug. 10, 2022

Illuminate Education Removed From Ed-Tech Privacy Pact Following Data Breach

David Saleh Rauf
Contributing Writer

You didn't think we would forget this one, did you?

Example #3

What happened?

- In early January 2022, the company identified unauthorized access to applications in its environment
- These applications hosted databases that contained PII from students including names, grades, behavior information, special education data, and demographic data.
- Ultimately, almost 2 million students across the country were impacted by the breach
- The company waited nearly two months to make its first notifications and went nearly radio silent after that

Example #3 - What Went Wrong

Communications

- Incident response is not an exercise in marketing
- The fastest way to snatch defeat from the jaws of victory is to try to spin your way out of a breach
- Be Clear, Be Concise, Be Transparent, State the FACTS!
- The technical response in these cases was great, but the overall response was a failure because of the communications problems

What Are the Takeaways?

Incident response for vendors is about competing priorities:

- *They want to protect their reputation and look out for their company's interests*
- *The "investigation" is often used as an excuse to avoid airing the bad news*

What Are the Takeaways?

Three things you can do to be ready to respond in the event of a 3rd party breach:

- **Strengthen Vendor Contracts**: include strict breach notification timelines, encryption mandates, and regular security audits.
- **Demand Data Encryption**: Recent incidents highlight the necessity for vendors to encrypt all sensitive data, both at rest and in transit, to mitigate the risk of exposure in the event of a breach
- **Shorten Notification Timelines**: the importance of rapid vendor communication and proactive incident response to limit harm to affected individuals and maintain trust cannot be overstated

Data Breach Reporting

Consider calling PTAC!

We can help by providing:

- *Technical Assistance*
- *Access to resources*
- *Training*
- *Moral support and virtual hugs…..*

We have all been there, and we really want to help!

Had a Breach? Got War Stories?

Don’t be Shy… Let’s Chat!

Data Breach Resources

Data Breach Response Checklist

https://studentprivacy.ed.gov/resources/data-breach-response-checklist

Data Breach Resources

Downloadable Data Breach Training Kits

https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings

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