Data Breach Awareness Exercise

NCES Forum, NESAC Committee

July 23, 2024

Ross Lemke
Privacy Technical Assistance Center (PTAC)

United States Department of Education
Student Privacy Policy Office

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

Structure of Today's Activity

- Review of data breaches in education
- Provide the Exercise Scenario Background
- Walk through the content and deliberate as a group on response activities
- Discuss best practices to reduce the risk of a data breach

Education is *THE* Target

- CISA and FBI issued a joint alert about directory traversal vulnerabilities that have affected schools and other critical services.
- In 2023, CISA and the FBI released a joint advisory about a vulnerability in PaperCut MF and NG that allowed actors to remotely execute malicious code without credentials.
- CISA published a report called "*Protecting Our Future: Cybersecurity for K-12*" to help schools reduce the cyber risk
- CISA partnered with the FBI and the MS-ISAC to publish a joint advisory about malicious cyber actors to targeting K-12 schools.

The Challenges

Remote learning & working is much more prevalent

- New technology platforms/software
- New reliance on enterprise systems, partners, vendors, and staff
- Staff training challenges
- New / Different attack surface & risks

Data Breach Scenario Exercise

Background

Your organization is partnering with the state university to perform a study including individual level student data to improve instruction and educational outcomes.

The research began two months ago, and your organization has been happy that already you are gaining insights into how you might make changes in curriculum to better student's education journeys.

Thanks, Freddy Foreshadowing
imgflip.com

Scenario Exercise – A Little Bump in the Road

Your CIO comes to work on Monday and her daily news feed headlines include a story about a crippling ransomware attack at the state university.

After spitting out her coffee, she quickly calls the data coordinator to find out if the researchers had called with information.

Let's Regroup – What do we know?

- Your organization has a strong infosec and privacy program
- Two months ago, the organization entered into a research agreement with the state university to provide research to improve student outcomes
- While the research has been going well, you receive information indicating that the university has recently been the victim of a ransomware attack

Question: What now?

A. Notify the incident response team

B. Call the researchers and ask what their status is

C. Book a flight – you always did like the Bahamas

Let's Put our Heads Together

Things to discuss:

- How can organizations set thresholds for incident response to ensure validation happens quickly without needlessly spinning up a full response?
- Should you assume the worst here?
- What are some best practices that you should have in place in your written agreements that could help here?

Scenario Exercise – Headache Confirmed

The data coordinator receives a call from the head researcher confirming your fears. The research team was affected by the recent ransomware attack and cannot currently access their systems.

They cannot provide assurance that the data sets were not accessed by the cybercriminals.

Question: Well, that escalated quickly. How should we react here?

A. Put out a press release to get ahead of the questions and tell the public that you are working with the university and will update them as the facts are known
B. Review the written agreement with the researchers to determine if there was a requirement for encryption at rest
C. Convene the Incident Response Team, notify your cyber insurance company, and refer to your incident response plan to understand what compliance requirements exist

Let's Put our Heads Together

Things to discuss:

- If the researchers can't determine IF the data was accessed, should you treat it as such?
- What if the researchers failed to adhere to the security requirements in the written agreement? Does that absolve your organization of responsibility?
- What role would state laws play in this situation?

Scenario Exercise – If there was a question

The university IRT reaches out to let you know that they have received notice from the cybersecurity firm that they hired to respond to the incident of some data leaked from the university.

It appears that some of the researcher data was made public on the group's "name and shame" website.

Scenario Exercise

The written agreement required that the data the researchers received was supposed to be encrypted at rest, but clearly this was not properly done.

Let's Regroup – What do we know?

- If there was any question, there isn't now. Your data was accessed.
- The ransomware group recently posted excerpts from the data set being used by the researchers on their website.
- This indicates that the data was not properly encrypted as specified in the written agreement.

Question: What is the best approach to take?

A. Request detailed information about what data was released and make a plan to notify the impacted individuals according to applicable laws
B. Annotate the disclosure in accordance with FERPA and make
C. Contact PTAC and self-report the incident to the Department of Education

Let's Put our Heads Together

Things to discuss:

- What recourse do we have if the researchers didn't follow our agreement?
- Should we notify law enforcement? What about our insurance provider?
- Should the university pay the ransom to protect your organization? Does that matter?

Scenario Out-Brief

- This incident is reflective of what is more and more a reality for local and state education agencies, incidents that occur entirely outside the agency's control in vendor or researcher systems
- LEAs and SEAs can address some of this risk by writing comprehensive written agreements that include provisions for audit, require proof of compliance, and use deidentified data where practicable
- Remember that incident response plans need to be extensible to a wide variety of potential incidents

Reducing the Risks

Tips for Safer Data and Stronger Response

This is your Party!

Things to consider when partnering with researchers:

1. Do they have acceptable levels of cybersecurity?
2. Who is your point of contact for incident reporting and response? Can you reach them directly?
3. Can you use de-identified data?
4. Does your agreement create an expectation of limited scope, responsible data use, and appropriate data destruction?

All of Us Are Targets!

- Most of the reported cyber attacks against K12 agencies were ransomware attacks
- Education currently accounts for more ransomware attacks than any other industry
- The pandemic has made us more likely to be attacked successfully and less likely to be able to operate through the event

Secrets to *less Painful Incident Response:

Let's Talk IR Secret Sauce

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

Leadership Driven

- Formal policy & plan
- Publicized and socialized throughout the organization
- Supported by reporting & feedback mechanisms
- Policy should assign roles and responsibilities, including leadership presence on IRT
- Absolutely NOT just an IT thing!

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 law enforcement & state entities

Communications is KEY

Think about including Public Affairs / Communications representatives in your IRT. Message is the often the hardest part of a response

- Ransomware & DDoS require some ‘splaining
- Need concise, clear, consistent messaging both internally and externally
- Frees up critical response resources
- Consistency of messaging conveys reassurance that the response is under control

10,000,000 STUDENT RECORDS YOU SAY...
LET ME CHECK ON THAT
imgflip.com

Would you like to play a game?

Threats evolve, so should your Incident Response plan!

- *Periodic risk assessments*
- *Annual IR exercise*
- *Involve third-parties, vendors, and partners*
- *Use as an opportunity to talk to law enforcement, cyber-insurance reps, contractors, etc.*

Tabletop Exercises

Simulated incident response based on carefully selected scenarios, where the IRT sits down and walks through a response.

- Build IRT cohesiveness and confidence
- Establish lines of communication
- Identify problem areas and streamline the IRP
- Ensure process and plans are extensible to the widest spectrum of incidents

Feedback Loops

"The most neglected part of the incident response plan is the part where you remember all the mistakes you made and fix them for next time"

-Me

Feedback Loops

Every organization should document their process and capture important data for process improvement:

- *What worked well?*
- *What didn't work at all?*
- *Did we miss something?*
- *What can we do better?*

Final Food for Thought

- You should have an incident response plan in place and train to it
- Every organization should have some form of data privacy & security awareness training for all employees, at all levels
- Clearly understand the legal requirements for compliance with all applicable federal, state and local laws
- Consider calling PTAC, we can help!!!

PTAC Resources

- **Data Breach Response Checklist**

  https://studentprivacy.ed.gov/resources/data-breach-response-checklist
- **Downloadable Data Breach Training Kits**

  https://studentprivacy.ed.gov/resources/data-breach-response-training-kit
- **PTAC Student Privacy Training**
  - ***Videos*** - https://studentprivacy.ed.gov/content/guidance-videos
  - ***Online Training Modules*** - https://studentprivacy.ed.gov/content/online-training-modules

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