Data Breach Awareness Exercise

NCES Forum, PPI 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 education agency went through a major attack by the Vice Society ransomware group last year that brought the agency's enterprise to a halt. Resulting in lost data and several days of downtime.

With the event in the past, the organization has hired a third-party auditor to evaluate the organization's recent cybersecurity readiness focus.

Background

The auditor recently completed a comprehensive week-long evaluation of the organization's cybersecurity infrastructure and has developed a report with several findings.

In the out-brief for the audit, the auditor calls out a few of the key findings:

Scenario Exercise

The auditors call out that they have seen:

1. Multiple unauthorized uploads of student data to a popular AI service have been occurring over the past six months.
2. The uploaded data includes names, addresses, student IDs, grades, and other sensitive information.
3. Initially, it is found that three staff members were involved in uploading the data, believing it would improve efficiency without understanding the security implications.

Let's Regroup – What do we know?

- The organization was the victim of ransomware in the last year, so they refocused on cybersecurity and hired a firm to audit their improvements
- The auditor identified unauthorized use of third-party AI tools where PII was involved
- This behavior looks to involve a small number of employees using the service to increase quality and productivity

Question: What do we DO about it?

A. Block the AI service at the firewall and discipline the employees involved

B. Spin up the Incident Response Team and lock the organization down

C. Notify the Incident Response Team and begin an investigation to determine the facts

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?
- Does your organization approve the use of AI for work purposes?
- What are some of the initial steps in this investigation to quickly determine the impact?

Scenario Exercise

The incident response team reaches out to the AI provider and requests that they delete any data that was shared with them through the disclosures by the employees.

The AI provider tell you that they can remove the records of the queries made, but that the data provided was used to train the models underpinning the service. They cannot guarantee that the information is truly wiped from the service.

Question: So, what is the best way forward here?

A. Get documentation from the AI service, annotate the incident and close the investigation
B. Update that resume, use that vacation time, and peace out! #bahamasvacation
C. The IRT discusses these facts with leadership and legal to determine the right way forward to ensure legal/regulatory compliance

Let's Put our Heads Together

Things to discuss:

- What happens if you can't undo the leakage of information? Is that OK?
- How can organizations manage the risk of AI disclosures?
- Is it really a data breach if the service just used the data for training?

Scenario Exercise

As you continue to evaluate the logs, you discover that the usage was much more widespread than initially thought. Dozens of employees are using these AI tools, mostly for non-sensitive work, but none the less the potential for data exposure has multiplied.

Scenario Exercise

To complicate matters, it appears that word of the incident has reached the outside world.

The front office receives a call from a local reporter inquiring about the data involved in the incident and what the organization is doing to protect the privacy of individuals involved.

Let's Regroup – What do we know?

- Well-meaning employees have been using an AI tool for work purposes, sharing student PII with the service to speed up their work
- The AI provider deleted what they could, but can not say with certainty that the information is truly gone as these interactions are used for training future responses
- News of the incident has leaked out and you are receiving inquiries about the incident

Question: How do we solve this issue?

A. Leadership and legal determine the required compliance steps, make required notifications, and develop a statement that is transparent, concise, and non-speculative about the incident and what steps you are taking to ensure it doesn't occur again
B. Develop organizational policies on the use of AI and provide training for employees on the responsible use of AI tools
C. Annotate the potential disclosure

Let's Put our Heads Together

Things to discuss:

- Was this a data breach? Think about all the laws that might apply.
- Do LLMs trained on FERPA protected data, retain these data or is the data sufficiently deidentified in the process?
- As the use of AI tools increases across the industry, what can regulators and lawmakers do to make the use of this technology safer and more privacy protective?

Scenario Out-Brief

- This incident highlights a troubling trend in incident response, “What happens if we can’t know the extent of the leakage”?
- The move to the cloud means we need to rethink how our incident response process works, extend the boundaries of what we think of as the incident team, and focus on information sharing
- It’s important to remember that incidents happen in a variety of ways, your plans should be germane to any incident that occurs

Reducing the Risks

Tips for Safer Data and Stronger Response

Incidents are more common than ever!

- Education currently accounts for more ransomware attacks than any other industry
- Explosions in technology tools like AI and remote learning make it easy to make a mistake
- We are more dependent on technology, more likely to share data with third-parties, and exploded our data footprint

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

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