Data Breach Response:

The In's and Out's of Incident Response Planning

Ross Lemke
Privacy Technical Assistance Center (PTAC)

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

Data Breaches Happen

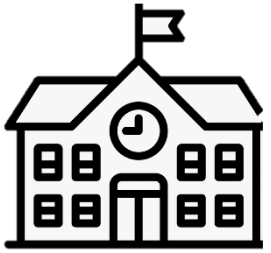
2022 Year in Review

- Hundreds of confirmed education data breaches
- Thousands of “other” incidents
- More than a dozen large breaches involving thousands of victims
- School closures in major cities
- Billions of dollars in costs for remediation

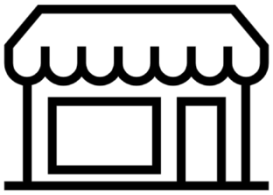
The Bottom Line

- 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**
- Incident Response Plans and processes better be tailored to meet these threats

Schools are not JUST Schools

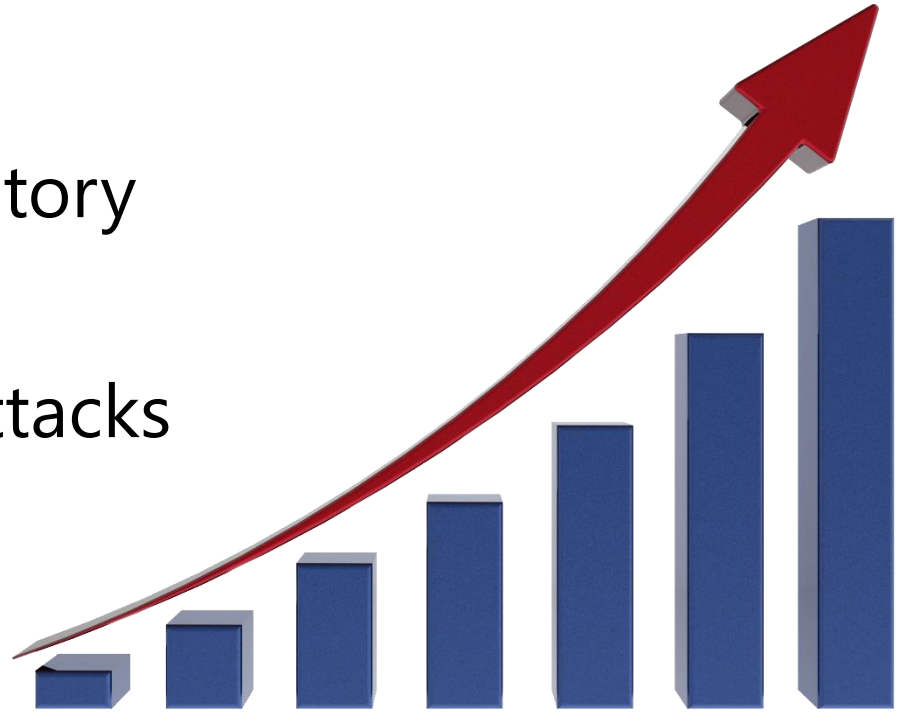


- More than just student data
- Health, family, financial data
- Employee data
- Sensitive Research data
- Other agencies' data
- Payment / Commerce data



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



Many Laws May Apply

- FERPA
- Higher Education Act (HEA)
- IDEA
- GLBA implications & other applicable financial laws
- State Laws

Building Robust Incident Response Capabilities

Data Breach Scenario Exercise

Background

You work for the Little Bend High School, which is a school of just over 700 students in a small suburb of a major metropolitan area.

In 2021, your high school fell victim to a ransomware attack that took down your school for a week and lead to a leakage of student data.

Background

Your school is currently part of a statewide effort to address school safety concerns through a program which attempts to identify students who are at risk for violence or self harm in order to provide resources and counselling before a potential issue occurs.

The state has provided grants to schools to help them conduct threat assessments and provide funding for early interventions and student support.

Background

Over the last few weeks, the school has worked with local authorities, vendors, and third-party contractors to review school records, public social media posts, and law enforcement records to identify students who may be in need of help.

The team has identified three students who meet the established criteria. Juan (junior), Brandon (senior), and Jennifer (freshman) are all students in your school who have red flags for a potential for violence or self-harm.

Background

Reports from the school safety task force indicate that Juan and Brandon are loners and have had a history of aggressive acts outside of school. Both have few friends and some discipline issues, as they have been involved in altercations at school.

Jennifer has been identified as being at risk for self-harm because of a clinical diagnosis of depression, coupled with social media posts about being alone and wanting to run away.

Background

- The team compiles their findings into a draft report and makes it available to school leadership and the lead counselor.
- The draft report needs to be reviewed and approved before any actions are taken and parents notified.

Background

Several days later you receive complaints from the parents of the students identified in the report. They say that your poor security practices lead to another data breach.

They claim that their children are being bullied and harassed online by their peers. Parents are threatening to sue the school, claiming that their children have been victimized by this disclosure.

What Now?

Clearly the information from the report has not remained confidential. What steps would you take to begin to address this situation?

Do you think that a data breach has occurred?

Consider:

- What is a data breach?
- Do you know enough to make any assertions at this point?
- What are your first steps to respond?

Where are we? Let's recap.

- Draft school safety assessment has been completed.
- Shortly thereafter, some students identified in the report begin being bullied by other students.
- Parents are livid that their children were included in the report and that the information got out.

Which is Best?

A. IT Director calls the safety task force and demands answers

B. Break out your incident response plan and convene the IRT to begin working the issue.

C. Panic, delegate a bunch of duties, then upload your resume to a bunch of online job sites

But Wait… You Have a Plan!

Because you attended the PTAC session on incident response last year, you have an excellent plan to deal with these types of issues.

The Event Evolves

You spin up your incident response team and begin to investigate how the information was made public. The report is saved on a secure file share, but the report was delivered via email to the principal and counselor. Several teachers and staff were interviewed in the process of creating the report, but all the interviews were in-person.

Your IT staff, still feeling the organizational trauma of the breach in 2021, begin examining the school network for signs of compromise.

The Event Evolves

The press is continuing to hammer at the school and the state government for what it calls "intrusive, Orwellian surveillance of students." The public is demanding answers as to what is going on at the school and how this information was made public.

Furthermore, since the data has been released, several parent groups are calling for the immediate dismissal of your IT Director following the second breach in two years.

Let's stop and think

Things to consider:

- Is this information covered by FERPA? Is this a FERPA violation or a data breach?
- Does the type of data impact whether it is a breach?
- What role do state laws play?
- Who should be involved in your response activities?

The Event Evolves

The principal was out of the office when the report was emailed. She was presenting at a State education conference. The school counselor recalls that he saved the attachment to his network drive and took a paper copy home to read after hours. He produces the paper copy complete with coffee stains and interspersed with his handwritten notes.

The principal read the document on her iPad at the conference over lunch. She sent a couple of emails to the counselor about her concerns about the report, suggesting redaction and questions about the recommendations in the draft report.

What Now?

We know who received the information, but there is no real indication at this point of a breach? What, if anything, do you tell the public at this point? Is this a Data Breach or a FERPA violation? Both?

Consider:

- What are you going to tell the press / public?
- What about FERPA? Was this part of the education record?
- Where will you take the investigation now?

Let's Discuss

- Two people at the school, the principal and the counselor got the email with the report
- The counselor saved it to his network folder and the principal viewed it online.
- The press and irate parents are breathing down your neck, and there are no immediate indicators of nefarious activity.

Lessons Learned From Incident Response

- Oftentimes the full extent of the issue is not known at the beginning of the incident
- Things can, and often do, get worse
- With student data involved – emotions tend to be heightened – parents have questions and want answers
- Incident response is not an IT problem – it is an everyone problem

IT Weighs In

IT completes it check of the logs for the email and file servers. There are no indications of unauthorized activity or access to the email accounts or files on the shared drive. The e-mails in question were sent to the correct recipients and were even encrypted in transit. The only access has been from school owned computers. Access to the file share was locked down, so only a select few school officials could access the report.

The principal had a call to the IT service desk about a problem with the wireless network, but it was resolved as a password issue.

Finally, a Break

The local news has printed a redacted image of the report on their website. However, they are unwilling to provide information on where they obtained the material beyond saying that they received it from an unnamed confidential source. You question all employees, and no one admits to leaking the document.

Finally, a Break

One of your school office staff recognize that the image in the paper shows a series of lines running down the printed page. The staff member shows you a document that they printed from the main office printer / copier just now which has the same pattern of lines.

Group Exercise: What Now?

So, the news says they received a printed copy, but they refuse to give up their source. An observant staffer notices a pattern that indicates that the leaked doc was printed at the main office. What do you do now? Does this indicate malicious activity? Do you update the public on this information?

Consider:

- How does this affect the investigation? Is this a criminal act?
- Do you call the authorities? If so, who?
- What steps will you take now? What can you do to mitigate the damage to the victims?

Let's Review

- The press has released a redacted copy of the draft report on their website
- Somebody printed the document the press has from the main office printer.
- The staff all deny any knowledge of the leak.

Wrapping Up

When you check the logs from the main office printer you find that the counselor attempted to print the report, but that there was an error because there was no paper left in the machine.

The counselor explains that he remembers the attempt to print but just figured that the printer was broken and printed from another printer on the other side of the office.

Wrapping Up

Meanwhile, in an effort to reduce the harm to the victims, you bring in the students who have been bullying the victims in for a talk. One of them says that another student named Terrance showed them the report and says that he found it laying on the printer in the office.

Terrance is a sophomore who is often in the office as an active member of the student council. When you ask him about the incident, he says that he picked up a stack of fliers from the printer and found the document. He viewed it his civic duty to let the public know about how potentially dangerous students were being allowed to continue to attend school. He provided the document to the local news station through email via their tip line.

Wrapping Up

So, it appears that a printer error triggered this whole incident. The activist student picked up the document by accident and provided it to the news believing himself to be a whistleblower.

Where does this leave the school?

- Is this a data breach?
- Who do you need to call / contact?
- Was a crime committed?
- How do you resolve this issue?
- What about the victims?

Scenario Out-Brief

- Here we focused on a different type of incident, one where we have very little influence on the response
- This is uncomfortable, because we all would like to think that we have more control over our own incident handling and remediation
- Exercises like this one force us to evaluate our planning and capabilities in non-typical situations

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

Start Strong….

- Not everything is a data breach (see legal counsel)
- Every response should begin by VALIDATING the incident
- Ensure the reports are correct and accurate
- Establish the basis of fact before you begin to throw switches and sound sirens
- Jumping the gun is as bad as being slow to react

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
- Data privacy & security awareness training for all employees, as well as contractors, researchers, and other 3rd parties
- 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