Data Breach Awareness Exercise

NCES Forum, TECH 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

You are a State Education Agency for the state of West Wiscarkansolina. As a state with many rural school districts, you struggle to get reporting in on time and face technological struggles as many of these LEAs use different technology platforms.

To solve this issue, you have provided a common secure file transfer service through a third-party provider, LeakyLinks Inc. Leakylinks is a Software-as-a-Service (SaaS) provider that allows all the LEAs to simply upload their large data files securely through the cloud.

Background

Schools use the system by uploading their reports and data files through the system using a web interface.

They find their school in the list of folders, open the uploads folder, and select the files they wish to upload. In addition to secure transfer, the system also archives the data and makes it available to users for review.

Scenario Exercise – A Little Bump in the Road

March 1st, 2024

A school admin reports that when they upload files, the timestamps appear to be wrong. A quick check of the archives appears to show all the files seem to have recent timestamps, even though they were uploaded some time ago.

They contact LeakyLinks customer support and open a ticket. LeakyLinks assures the LEA that it is most likely a bug and will have their developer shop troubleshoot the issue.

Let's Regroup – What do we know?

- The SEA uses LeakyLinks to provide a common secure file transfer capability for LEAs to submit reporting to the state
- Every school in the state uses this platform to upload and store their reporting data
- An LEA recently contacted customer support because they noticed problems with file timestamps

Question: Is There any "There" There?

A. No. These things happen all the time, let the company fix the bug

B. We're under Attack! Sound the alarms, wake up the boss.

C. Sounds sus… Let's have IT check out and see if its just that school or everyone

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?
- Is it better to have LEAs contact customer support themselves, or to run everything through the SEA?
- What could the SEA do at this point?

Scenario Exercise – Headache Confirmed

March 10th, 2024

Spurred by the recent timestamp issues, IT has been scouring the LeakyLinks logs and noticed some strange access patterns that suggest unauthorized access.

The SEA notified LeakyLinks and they launch an investigation which confirms your suspicions. These patterns suggest the system has been accessed by one of more unauthorized persons.

Question: What immediate steps does the SEA need to take?

A. Update that resume, use that vacation time, and peace out! #bahamasvacation

B. Notify the FBI, call your cyber insurance company, and notify the AG

C. Convene the Incident Response Team, integrate with LeakyLinks for threat data exchange, and brief leadership & legal

Let's Put our Heads Together

Things to discuss:

- Once everyone is briefed, what are the first things we need to do?
- How do state laws impact what happens in the early stages of a response?
- What parties should be a part of the incident response process? Who should the SEA notify?

Scenario Exercise – The Proverbial Cat is out of the Bag

March 15th, 2024

LeakyLinks confirms to the incident manager that their investigation shows that hackers successfully exploited a previously unknown 0-day in their platform to gain access to potentially all of their customers data, including the SEA and all the LEAs.

They are not able to quantify what particular data was viewed or accessed, but they say the attackers could pretty much “see everything”.

Scenario Exercise

To complicate matters, word of the incident has reached the outside world. The front office has begun to get calls from reporters from various districts asking questions about the incident and what the impact was.

Let's Regroup – What do we know?

- LeakyLinks discovered that hackers exploited a 0-day in their software that allowed unfettered access to files in the system
- Currently unable to quantify the extend of what was accessed, but potentially all data in the system was affected
- News of the incident has leaked out and you are receiving inquiries about the incident

Question: Is this our problem, and what should we do about it?

A. Well, this sounds like a whole lot of not my problem… LeakyLinks needs to deal with this.

B. Make notifications to LEAs, coordinate facts about the incident and promulgate points of contact to control messaging and ensure facts are presented accurately.

C. Incident Team coordinates with leadership, legal, and communications to develop clear messaging to be transparent, concise, and non-speculative about the event

Let's Put our Heads Together

Things to discuss:

- What is the best way to handle the questions and outcry? What notifications and support should be offered to impacted individuals?
- What could be the potential legal or regulatory impacts of this incident?
- What does the potential loss of integrity of data mean for reporting? What can the SEA/LEA do to ensure the integrity of data?

Scenario Exercise

Along with LEA reporting data on students, the attackers were also able to access the credentials and profile information of the users at the SEA and LEAs.

LeakyLinks warns that they are receiving reports from other customers that they are being targeted with spear-phishing attacks.

Let's Regroup – What do we know?

- In addition to student data, the attackers also has access to login and profile data for the system users themselves
- Other clients of LeakyLinks are receiving sophisticated phishing attacks targeting their users who had access to LeakyLinks

Question: How should we address this incident?

A. Craft a notification for all LEAs and SEA employees notifying them to change their passwords immediately in the LeakyLinks system and to be on the lookout for suspicious emails

B. Just force a password change, you have phishing training and spam filters to protect the users

C. Get more information on the phishing mails from LL, provide this information to the LEAs so they can inform their users and create signatures in their email filters

Let's Put our Heads Together

Things to discuss:

- Was this a data breach? Think about all the laws that might apply.
- Is there anything the SEA/LEA could have done to mitigate the impact of this attack?
- This highlights the importance of written agreements in protecting student data. What elements can/should you put in your written agreements to bolster cybersecurity & incident response?

Scenario Out-Brief

- This incident is reflective of what is more and more a reality for education agencies, incidents that occur entirely outside the agency's control in vendor systems
- 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
- Its 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

Are you partners, or Partners?

Things to consider when partnering with vendors:

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. What assurances do you have that the vendor will notify you of any issues? What is in the SLA?
4. What is the vendor's track record, have they been involved in a recent breach?

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

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