Data Breach Exercise

Utah Privacy Workshops
November 4-6, 2019

Mike Tassey
Data Security Advisor
Privacy Technical Assistance Center

Agenda

- Introductions
- Group Assignments
- Scenario Background
-  MAGIC HAPPENS
- Review & Discuss

Introduction

- Think of this as a “murder mystery dinner”
- Today we will navigate a fictional scenario and work together to identify key steps for response and recovery
- Assume the role of responsibility as leaders of the organization
- This exercise will expose you to a scenario which has the potential to be a data breach
- You must work together to develop appropriate steps and messaging (both internal & external) to address the scenario as it unfolds

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.

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. The state has provided significant funding and resources to perform a study to see about its effectiveness.

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 organization 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

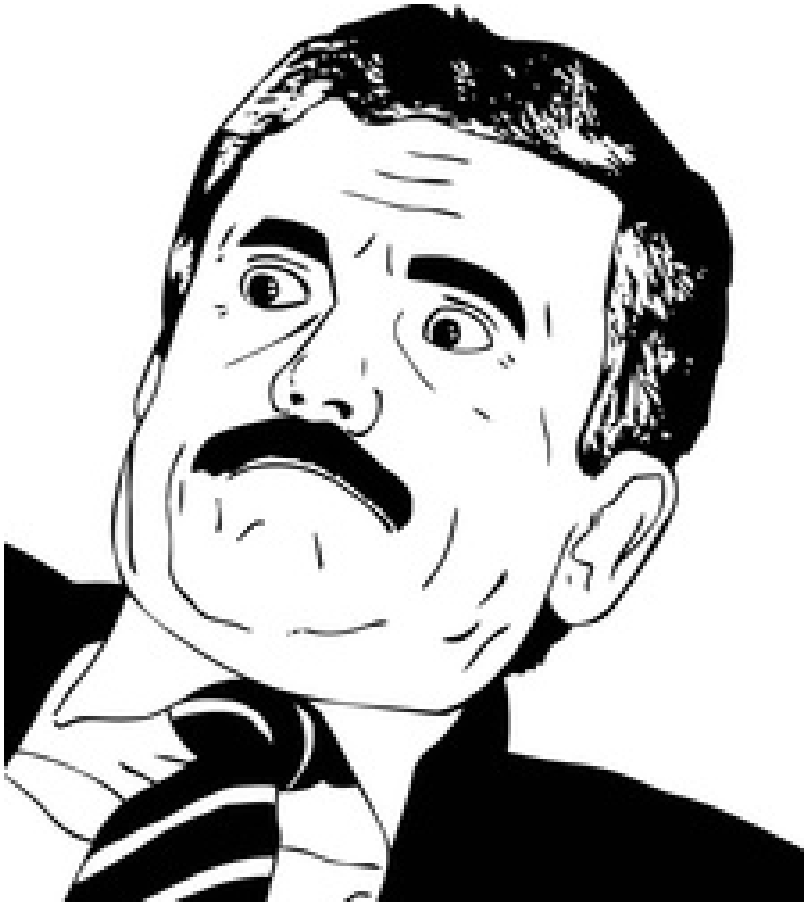
Reports from the school safety task force indicate that Juan and Brandon are both loners, with a fascination with firearms. Both have few friends and some discipline issues as they have been involved in some altercations at school.

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

Several days later you receive complaints from the parents of the students identified in the reports about why their children were included in the report.

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.



Group Exercise: 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?

Talk It Over

10 Minutes

Where are we? Let's recap.

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

The Event Evolves

You begin to investigate how the information was made public. The report was delivered via email to the principal and counselor. Several teachers and staff were interviewed in the process, but all of the interviews where in person.

The press is continuing to hammer at the school and the state government for what is 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.

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 copy home to read after hours. He produces the paper copy and it has coffee stains and is interspersed with his handwritten notes on it.

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 highlighting issues with FERPA regarding the school maintaining information like this as part of the record.

Group Exercise: 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?

Talk It Over

10 Minutes

Let's Chat

- 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 is breathing down your neck, and there are no immediate indicators of nefarious activity.

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 file shares. The only accesses have been from school owned computers.

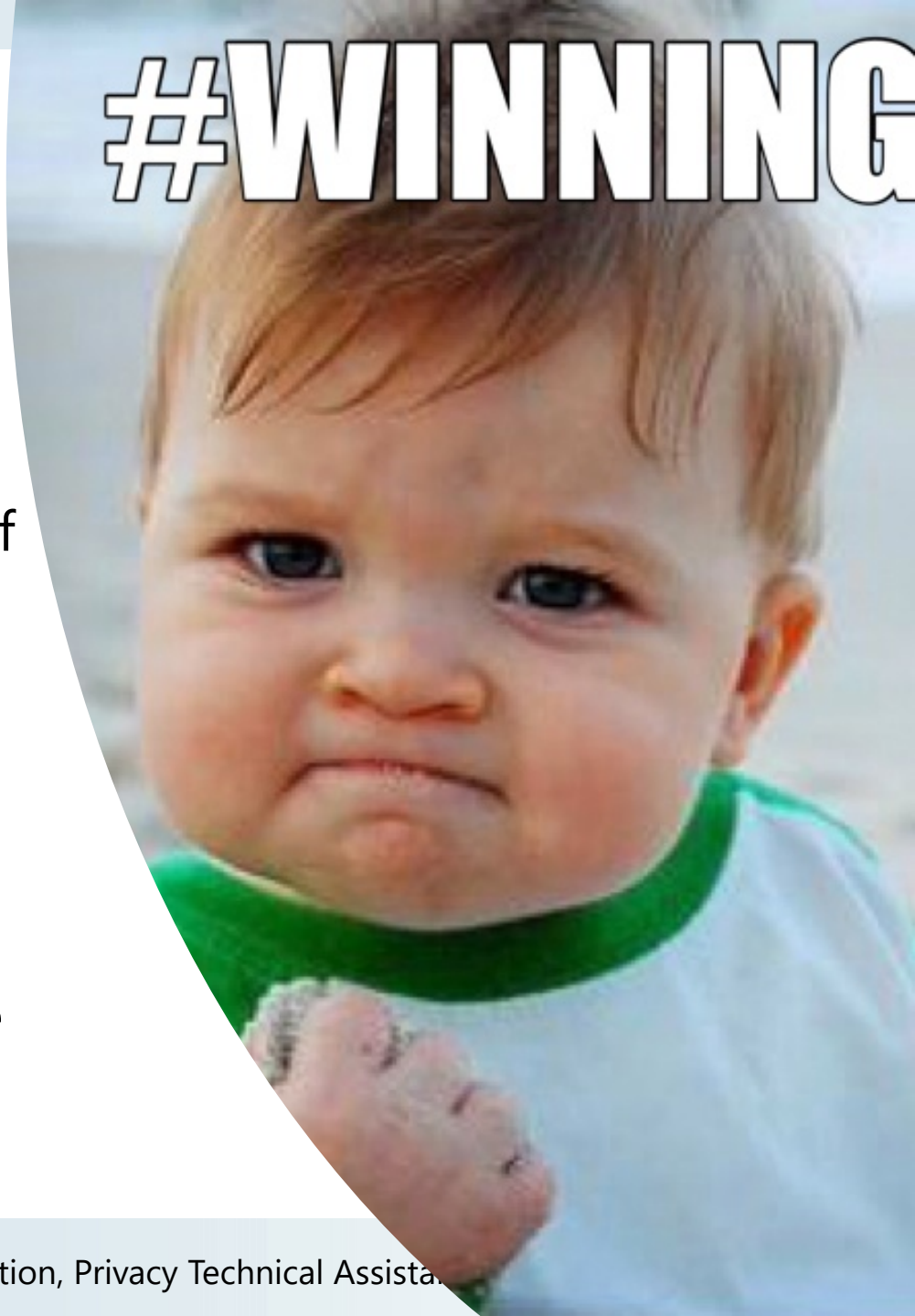
The principal had a call to the IT service desk about a problem with the wireless network, but it was resolved as a password issue.

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 a unnamed confidential source. You question all the 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?

Talk It Over

10 Minutes

Let's Chat

- 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 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?**

Let's talk about our plans

Who wants to go first?

For More Information

PTAC website @ https://studentprivacy.ed.gov

Resources include:

- Data Breach Response Training Kit
- Breach Response Checklist
- FERPA Online Training & videos
- Recorded Webinars

Contact Us:

PrivacyTA@ed.gov / 1-855-249-3072

ADA Compliant 11-19-19