Data Breach Awareness Exercise

Vermont

Ross Lemke
Privacy Technical Assistance Center

United States Department of Education
Privacy Technical Assistance Center

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

Where We Stand

- 350+ breaches in the last three years
- Millions of student & staff records compromised
- Increased focus for W2 scams, ransomware, and incidents related to remote learning
- Education is no longer unknown to the bad guys
- FBI has issued several advisories warning of targeting by cyberattacks specifically at schools

The Challenges

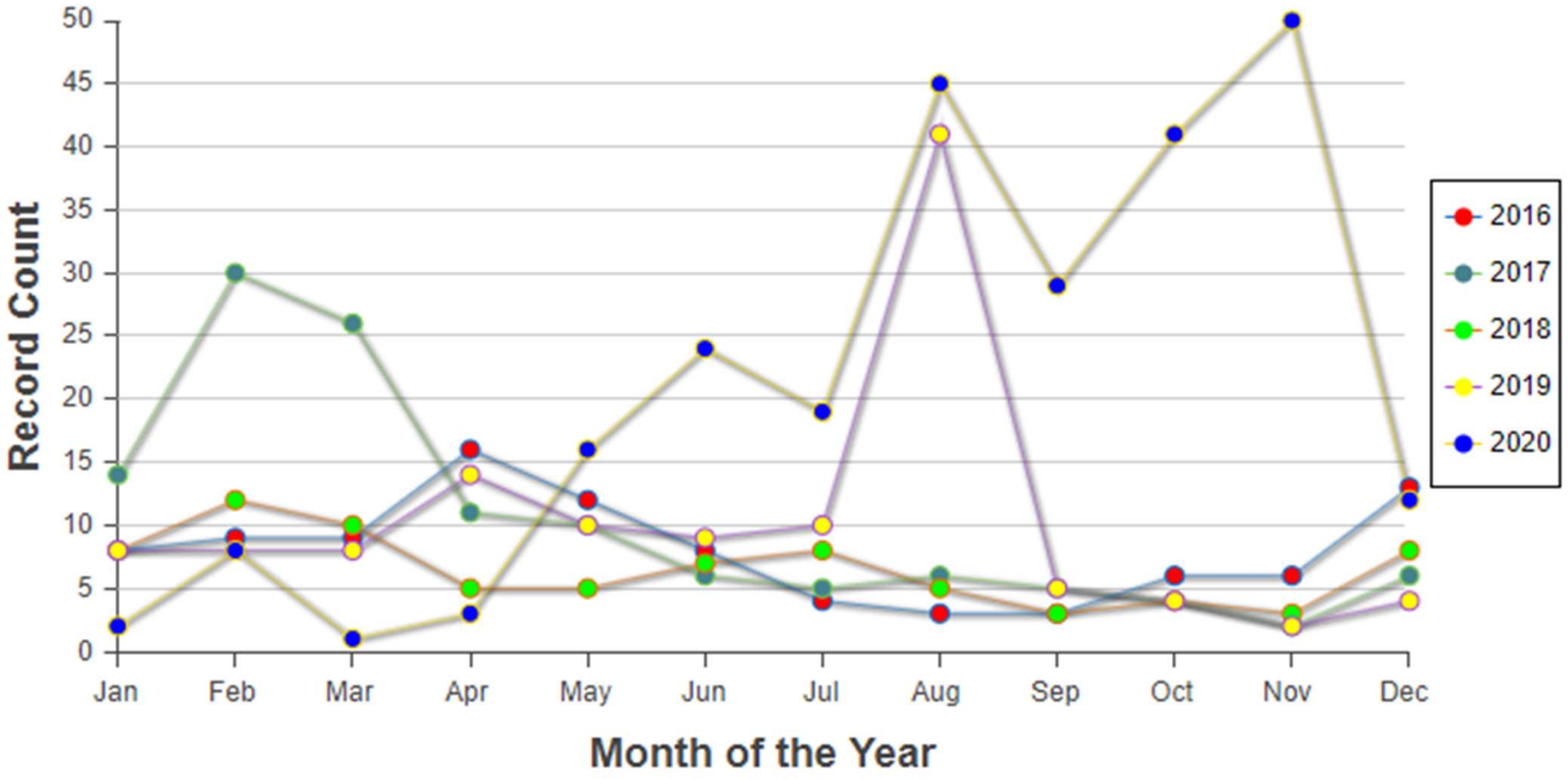
Remote learning & working is much more prevalent

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

Reported Data Breaches in Schools

United States Department of Education, Privacy Technical Assistance Center

How does this translate to schools



* Source: Identify Theft Resource Center (https://www.idtheftcenter.org/)

Problems in ED Data Systems

- A ton of old or unpatched software
- IoT devices in schools include:
  - Server room cameras & sensors
  - School surveillance systems
  - Access card readers
  - Modems (UPnP hackable)
  - HVAC / Boilers
- Hundreds of forgotten servers / computers
- Passwords
- Vendor vulnerabilities
- People

Data Breach Scenario Exercise

Introduction

- Think of this as a group led exercise for your incident response plan
- Think of this from a wide perspective, take a wide view and consider all the angles
- At the end of each segment, and along the way, we will be presented with a series of questions *(like a choose your own adventure novel)*.
- Don't be afraid to challenge the answer… this is an exercise in navigating the incident

Background

You are employees of the *Nosutch County Public School District*. This is a very large school district with 40,000 students in 35 schools (elementary, middle and high schools)

- ***4000 Employees***
- ***Centralized IT services & support***
- ***Schools have limited IT***
- ***Annual risk assessments***
- ***IT audit last year***
- ***Recent security scan of public accessible systems***

Background

The district prides itself on its online employee service portal where employees can review or change their payroll information, update & manage their employee information, view and request leave, and review employment documents.

The district has a variety of service partners which provide services like learning services, email and cloud, payroll and business process services.

Scenario Exercise - Game on!

Last Friday was payday, today is Tuesday and some teachers and staff are calling complaining that their paychecks have not been received.

The district uses a payroll processing company to disperse employee pay. No problems have been reported so far.

Question: What is the first step here?

- Call the police and report the stolen funds.
- Call the payroll provider and initiate a breach response to lock down the system and notify leadership.
- Review the system logs and configurations, validate the information from the complaints.

Scenario Exercise

It appears that over 100 employees' direct deposit information has been recently changed to reflect accounts that don't belong to the employees.

All the staff denies any knowledge of the accounts being changed.

The accounts were all changed to the same three account numbers on the same day on or about the same time.

Scenario Exercise

The payroll company confirms that the transactions in question have gone through. The money (totaling $256,000.00) has been debited from the payroll account and deposited into the accounts in question.

Question: What is the best response?

- Initiate the incident response process and convene the incident response team. Assign an incident manager, coordinate with leadership and open lines of communication with partner providers.
- Since there was a breach, the CIO takes charge and turns off access to employee portal, notifies the authorities, and begins to prepare to notify the affected employees.
- Contact the payroll provider and have them re-issue paper checks for the affected employees. Prepare a press release explaining the issue.

Let's Regroup – What do we know?

- Employee direct deposit information for some employees has been changed by an unknown actor
- The accounts were all changed to reflect one of three different accounts
- Funds have been dispersed to the accounts in question totaling $256,000.00

Put Your Heads Together

Things to discuss:

- Do you call this a data breach? Why?
- What does your state require you to do in a data breach?
- Who is involved at this point?
- Do you make any statements? If so what messaging do you use?
- What steps can you take to stop the bleeding?

Scenario Exercise

It is now Wednesday and your staff has examined the system logs and identified that all the affected accounts were accessed over a 9 hour period from the same internet IP address belonging to an Internet Service Provider in Sao Paulo, Brazil.

Question: How did this most likely happen?

- Hackers guessed the credentials of 100 employees who had weak passwords.
- Thieves found a hole in the portal's security, allowing them to bypass authentication and access critical employee data.
- The users fell victim to some kind of social engineering attack.

Scenario Exercise

None of the employees or staff can recall receiving anything that seemed like a phishing email.

All staff are required to take phishing awareness training annually as part of their annual training requirements.

Question: Where do we go from here?

- Wipe the affected employees' computers and reinstall the software to a pristine state and require the employees to change their passwords, or;
- Disconnect the employees' computers from the network and examine them for evidence of malicious software or phishing emails, or;
- Temporarily disable all employees' access

Scenario Exercise

The IT staff, along with security contractors brought in to assist, have identified no malicious software on the employees machines, but they have identified suspicious connections occurring from a server in the data center. It appears that this machine has been sending and receiving data over HTTPS (Port 443) to an IP address in *Brazil*.

Scenario Exercise

The machine is a database server which provides services for the computer science classes at the district's high schools. Student's use remote desktop to access the server with administrative privileges in order to complete labs where teams build data driven web applications as part of their semester project.

Let's Regroup – What do we know?

- Employee direct deposit information for ~100 employees has been changed by an unknown actor
- Victims portal accounts touched from an IP in Sao Paulo, Brazil
- Around the same time a district server is talking to Brazil

Put Your Heads Together

Things to discuss:

- Have you called the police? Why?
- What is your plan of attack for the server you found beaconing?
- Now that you have more information, do you make a public statement?
- What accommodations are you making to get your staff paid?

Scenario Exercise

It is now Thursday. While examining the server, your staff finds that the server still hosts the back-end database for a now defunct student project from last year.

It is an application which allows real time chat between users like a chat room, but users can also share files and create profiles.

It was very popular with the staff and teachers alike before it was taken offline prior to the systems audit at the end of the year. This application's authentication mechanisms used unsalted MD5 hashes to protect user's passwords in the database.

Question: How does the server information change things?

- The server may be the vector the attackers used to get the staff portal passwords
- The server gave the attackers a jumping-off point to attack other servers in the organization
- The server likely has student information on it, resulting in a potential FERPA violation

Scenario Exercise

The MD5 hashing algorithm is very insecure. Coupled with the fact that no additional salt was added means that these passwords could be easily cracked.

An attacker who has access to this database would be able to reverse engineer these staff passwords. If the staff did what they are not supposed to do and reused passwords across applications, the attacker would be able to access their other accounts.

Scenario Exercise

Analysis of the database hashes along with input from the victims (*asking them, is this your password*) has shown that every victim had an account on the application, and every victim answered in the affirmative when asked if their cracked MD5 password was their employee portal password.

So we now know where the attackers got our passwords, now how did they get onto that server?

Press Release: You get a call from the press about a data breach. What is your message?

Think About:

- Clarity and brevity
  - Content
  - Delivery

Scenario Exercise

Log analysis and correlation shows that a particular junior, Joanna Smith, was logged in at the time of the first connection to the IP in Brazil.

When questioned, she says that she was logged into the server and browsing a developer forum for payment processing code for her project. Someone responded to her question with a link to the code that she needed, and she clicked it. Unfortunately the link took her to a site which installed malicious code known as a Trojan Horse instead of the tool she was looking for.

Scenario Exercise

The malcode connected back to the attacker and enabled them to control the computer with the same permissions as the user, which in Joanna's case was as an administrator.

This access enabled the attackers to read the database containing the staff passwords. The attackers were then able to simply log in to the staff portal using these passwords.

Wrap Up & Review

- Next steps?
- What could the district have done differently to avoid this?
- Would this be considered a data breach in VT?
- What are some lessons learned or best practices we can take away?
- How can this exercise be made better for you?