



Data Breach Awareness Exercise

METIS

July 17-19, 2019

Ross Lemke
Sean Cottrell
Privacy Technical Assistance Center

United States Department of Education
Privacy Technical Assistance Center

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!




WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.

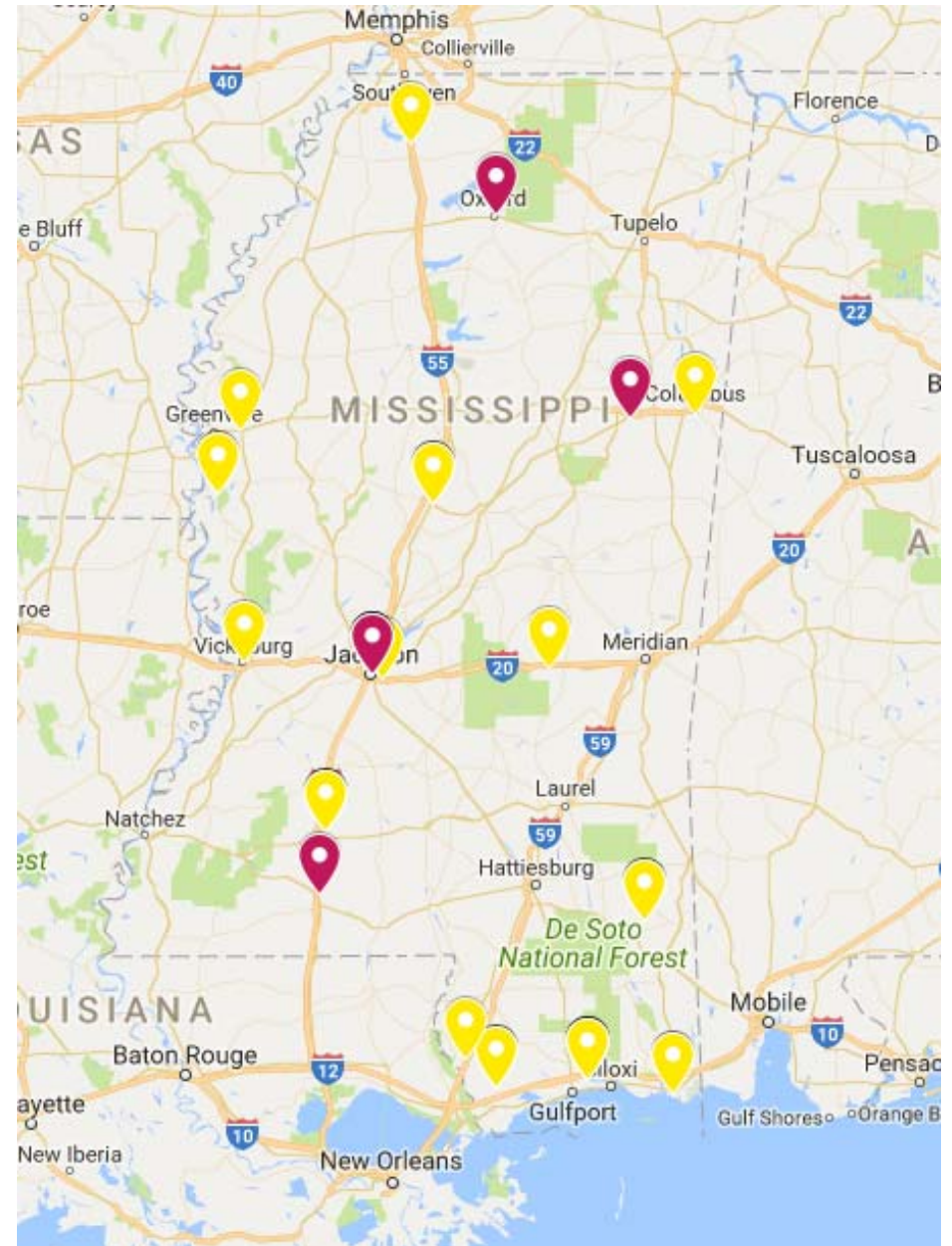


Agenda

- Introductions
- Group Assignments
- Scenario Background
-  *MAGIC HAPPENS*
- Report Out & Discuss

MS Breaches & Defacements

- Over 40 Breaches and Defacements
- Multiple countries:
 - *Algeria*
 - *Turkey*
 - *Indonesia*
 - *Saudi Arabia*
 - *Turkey*
 - *US*



Defacements

A black rectangular area with a starry background. The text "hacked by Hmei7" is centered in white. The stars are small white dots scattered across the black field.

hacked by Hmei7

Hmei7



- Aditya P. Mikael
- Web Developer, Programmer
- Malang City, East Java, Indonesia
- Facebook:
<http://www.facebook.com/n1cedre4m>
- Personal Facebook :
<http://facebook.com/petaniweb>
- Twitter: @HaloAdit, @PetaniWeb

SEJEAAL

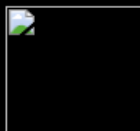


Memorial Of Gaza Martyrs.

Hacked By Smail002



DZ-SEC



::| Contact :: dz4all@live.fr |::



00X - yasMouh -kader11000- Damane2011 -AnGeL25dZ -ra3ch -?Ev!LScR!pT_Dz -mztol-dz -crvi_dz - The MaSk - The MaSk

(c) 2011 by www.dz4all.com/cc



Hacked By Mujahideen Hacking Unit

[Protest Page]

- On 9/11 the USA Government Crashed a plane into the Twin Towers and blamed it on Muslims, On October 7, 2001 the American & British Government declared a war on Afghanistan, yet they have still failed to find Osama Bin Laden but have managed to kill over 32,000 Muslims. - On March 20, 2003 the American & British Government invaded Iraq, they killed 16,000 Muslims just for Oil - Ev



MORE VIDEOS

▶ 🔊 0:00 / 3:46

⚙️ YouTube 🗄️

Mississippi: Testing Breach Exposed Data From 663 Students

Mississippi education officials say a data breach at testing vendor Questar Assessment exposed information for 663 students in Tupelo and Jefferson County.

Jan. 22, 2018, at 8:25 p.m.



AP

JACKSON, Miss. (AP) — Mississippi education officials said Monday that a recently disclosed data breach by a testing vendor has exposed information from 663 students in Tupelo and Jefferson County.

State Superintendent Carey Wright said that Questar Assessment believes an unauthorized user gained access to records from 2016 tests for 490 students at Tupelo Middle School, 72 at Tupelo High School and 101 at Jefferson County Junior High on Dec. 31 or Jan. 1.

The Mississippi Department of Education plans to send letters to every student affected.

The unit of New Jersey-based Educational Testing Service has told New York officials that 52 students there had data exposed, in a data breach that happened at about the same time.



MDE: School district website contained students' personal info

Three school districts affected by data breach

Published: Monday, April 16, 2018, 2:10 pm EDT
Updated: Wednesday, September 11th 2016, 6:42 pm EDT



23 Lamar County School District employees had personal information compromised after a system data breach. Source: Alabama News Network

LAMAR COUNTY, MS - Three school districts in the area are experiencing a security breach of their employees' personal information.

To far Lamar county, Marion County and the Columbia school districts are having these issues.

According to Lamar County Superintendent Tess Smith, the district uses a company called INNOVAK that allows staff to access its pay stubs and W2's through the internet.

Smith said 29 employees in the Lamar county school district were affected.

Other districts in Mississippi like Columbia are dealing with the same problem. About 20 employees from the Columbia school District were affected. Marion County school district, 12 were affected.

The FBI and IRS have been notified and are working to resolve the issue, according to Smith.

"For it to happen to us, yeah it was surprising and very disappointing," Lamar County School Board President Mike Pruitt said.

According to INNOVAK, the breach was only related to employee W2s, and no other information was accessed.

Smith said INNOVAK has locked down the portal, and precautions and safety measures have been put into place.

The staff was given detailed instructions on how to proceed, and are working with INNOVAK and the IRS in order to assist the affected employees, according to Smith.

About four employees from Marion County schools and one from Lamar County had their tax returns rejected.

Copyright WQAM 2016. All rights reserved.

Data Breaches in the News

- Mississippi testing vendor breached
- Affecting two districts and three schools in the state
- Other states affected as well

Structure of Today's Activity

- Introduce how the Scenario Works
- Assign Groups
- Provide the Scenario Background
- Group Deliberation
- Report and Discuss



Data Breach Exercise

- You will be divided up into a number of groups, depending on the group you may be either a K-12 organization or part of a Postsecondary Institution
- Each group will 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

First I was like



Then I was like



But then I was like



Suggestions

- Think about each of the roles needed in your organization (e.g., public information officer, data system leadership, attorney, auditors, etc.).
- The full extent or impact of a data breach is rarely known up front. Do your best to anticipate what might happen, but don't get ahead of yourself.

District Data Breach Exercise

Each team will develop two key products:

**1. Public and Internal Communications/
Messaging** – Develop the message(s) you will deliver to your staff, students, other state agencies, the media, and the public.

District Data Breach Exercise (cont.)

2. Response Plan – Outline how the district will approach the scenario and what resources you will mobilize. Describe who will compose your response team. Identify goals and a timeline for your response.

Background and Scenario

South Westerland School District

- ~6000 students
- 5 Schools
- Decentralized IT with schools managing their own IT infrastructure
- SIS is at the district

Westerland Area Community College

- ~4200 students
- 2 campus sites
- Centralized IT managed from main campus
- Records & Admissions at each campus

Background and Scenario

Daniella Smith is a 17 year old high school senior who is currently dually-enrolled in at the Community College for advanced mathematics courses for which she will receive credit.

It is now the end of May and she has recently completed Calculus II and she is looking to matriculate in the Fall Semester at the College.

Background and Scenario *(cont.)*

The High School has requested her grades from Community College so that she can receive credit towards her graduation requirements.

The school maintains a close partnership with the College and to facilitate faster data exchange has implemented a file transfer system which is shared by the two entities and managed by the local school district.

Background and Scenario *(cont.)*

Daniella's parents call the school and complain because their daughter is being cyber-bullied on social media by her former classmates about failing her final exam in Calculus II.

Daniella denies having any trouble with Calculus II and doesn't understand how this could happen as she is sure she did well on the final exam. She is heartbroken that her reputation as a perfect student has been sullied.



Okay, What Now?

1. Go over the background and scenario carefully. What do you know? What don't you know?
2. Begin considering your approach to a response. Elect a team member to take notes.
3. We will regroup in 10 minutes. Be prepared to talk about next steps and rationale

District Data Breach Exercise

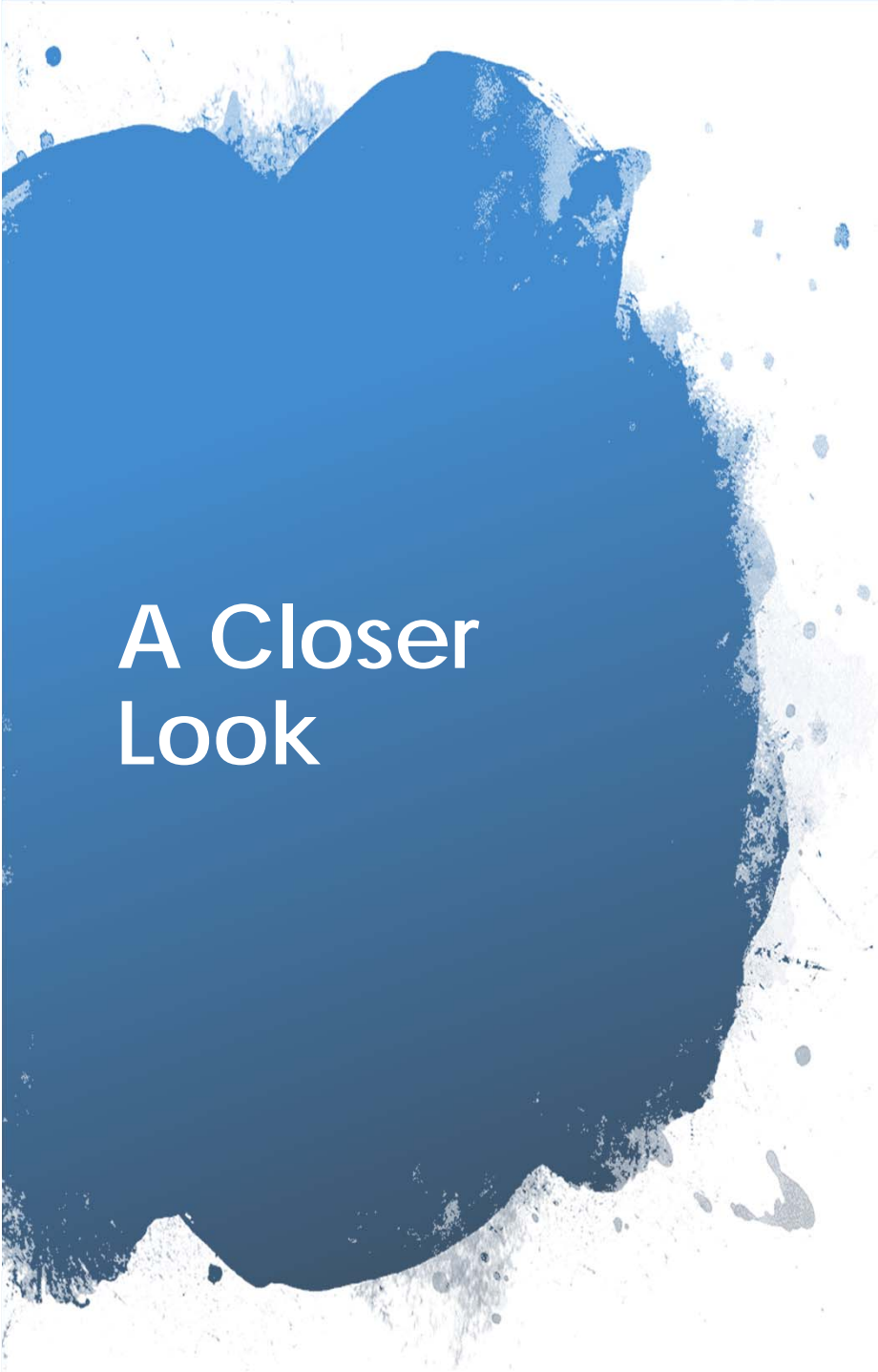
10 Minutes



Time to Regroup!



Let's discuss each group's approach to a response.



A Closer Look









A look at the transfer site reveals nothing out of the ordinary, it seems that the transfers occurred as normal.

The site requires a username and password to log in. Only certain approved users at the District and at the Community College have permissions to access the file transfer server.

Index of /

Not secure | ftp://216.100.88.219

Index of /

Name	Size	Date Modified
 Enrolled Students.csv	5.7 MB	8/20/17, 7:58:00 AM
 student_transcripts		6/3/18, 3:42:00 AM
 Fall Semester - 2017.xls	10.5 MB	12/5.2017, 1:37:00 PM
 banner.txt	94.5 kB	8/5/16, 9:32:00 AM
 feedback-forms.zip	122 kB	11/13/17, 10:45:00 AM
 Spring Semester - 2018.xls	23.6 MB	5/28/18, 2:14:00 PM
 Summer Semester - 2018.xls	86 B	6/14/18, 7:05:00 AM
 readme.txt	681 B	3/23/16, 4:02:00 PM



The Professor

- Daniella's professor for Calculus II weighs in and confirms that Daniella did not in fact fail her final exam... in fact she had a perfect score!
- She confirms that the grades in her book reflect the correct grade and is unable to explain why the grades differed between the College and School District.
- John, who is the person responsible for sending the records to the District also confirms that the grades are correct in their system.



What a Quandry!

1. Is this a matter that is of concern? Or just a mistake? What could be going on here?
2. How could records differ so drastically between the organizations? Should you address this as a security incident? If so, at which organization?
3. What steps should you take next? Be specific.
4. What do you tell the parents?
5. We will regroup in 10 minutes. Be prepared to talk about next steps and rationale

District Data Breach Exercise

10 Minutes



Time to Regroup!



Let's discuss each group's approach to a response.



A Closer Look

- In the course of the investigation it is determined that John's account logged into the file transfer site and replaced the existing transcript file containing Danielle's grade some time after the official transcript file was sent
- Copies of the original file show that the grades were initially correct and were then changed when the subsequent file was uploaded a few days later

What a Coincidence

- The online bullying began the day after the second file was uploaded to the transfer server
- Two of the main perpetrators of the bullying on Danielle's social media account are computer science majors who are also in her Calculus II class, with somewhat less stellar grades
- One of the two is a student worker assisting in the IT department
- Logs from the affected server show that the accesses came from two different IP addresses, the first one at the college and the second from the local campus coffee shop





Things to Consider

1. Is there foul play here? What, if anything, can we do at this point?
2. Since the bullies seem to know Danielle's grades, is this a data breach? Whose responsibility is it, the district or the college?
3. Do the facts yield a clear picture of what happened? What can you tell Danielle's parents?
4. What steps should you take next? Be specific.
5. We will regroup in 10 minutes. Be prepared to talk about next steps and rationale

District Data Breach Exercise

10 Minutes



Time to Regroup!



Let's discuss each group's approach to a response.



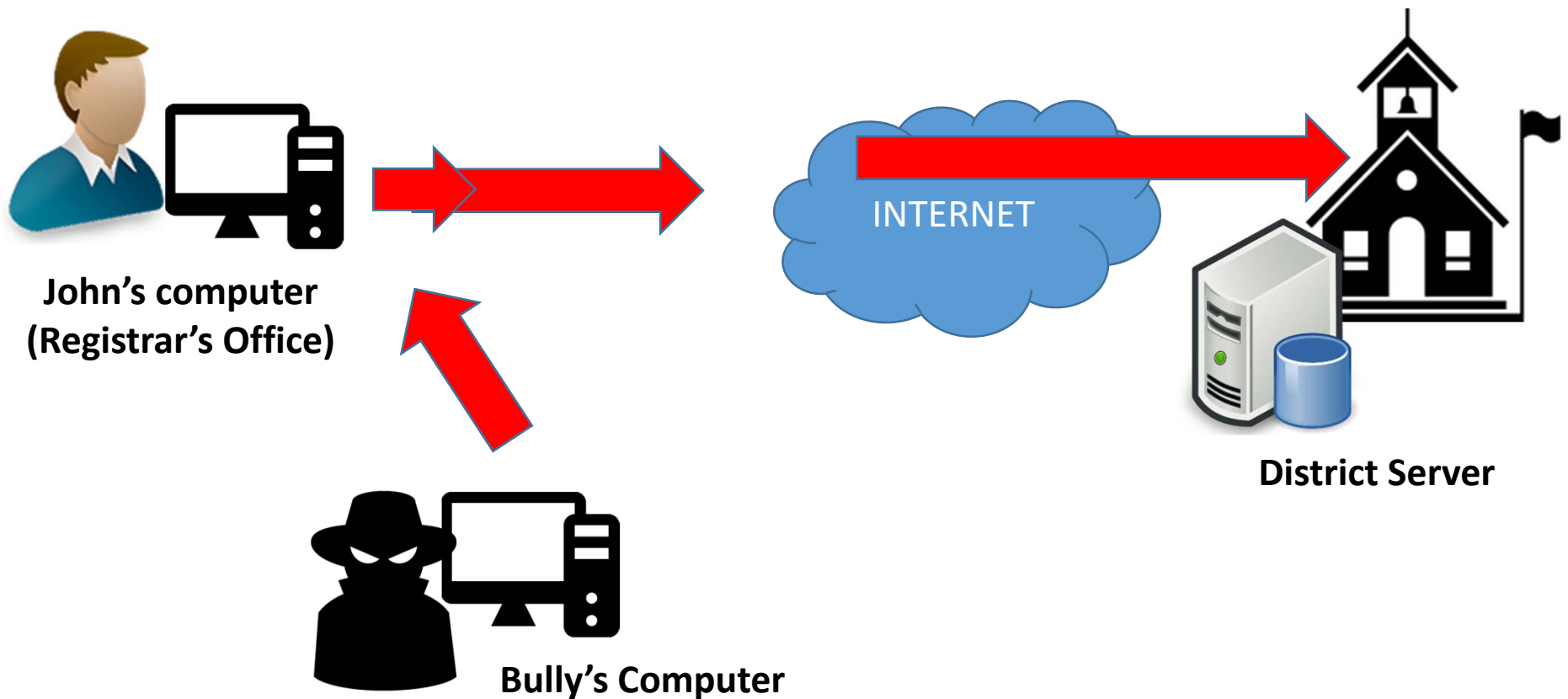
A Closer Look

- Investigators at the community college question the students responsible for the bullying. One of the two admits that it was a prank to get back at Danielle who is much younger and getting far better grades
- The cooperating bully explains that his friend performed a “Man in The Middle” attack on the registrar’s office network. This enabled them to sniff the authentication portion of John’s session with the school district’s file server and get his password
- They then used that information to access and change the file John placed on the server, re-uploading it with altered grades



The MiTM Attack

Unencrypted Password



No Honor Among Thieves

Well, our canary is singing and it appears that this is all a juvenile prank played on Danielle by some classmates who were made to look bad by her skill in Calculus.

- *Is this a data breach?*
- *Can Danielle's parents make a FERPA complaint? Against which organization?*
- *Depending on what organization you are representing, what are your next steps?*



Wrapping Up

- The attack happened at the College, but the system was at the District. Who had the breach?
- Has a crime been committed? Do you contact the police?
- Is this a Data Breach in your state? Keep in mind that data breach is a defined term.
- Just having a password is not enough. What could have either organization done to avoid this situation all together?



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

