# Data Breach Awareness Exercise

## Arkansas Department of Higher Education

## March 2018

**Mike Tassey**
Privacy Technical Assistance Center

# Structure of Today's Activity

- Introduce how the Scenario Works
- Assign Groups
- Provide the Scenario Background
- Simulation & Group Discussion
- Report and Discuss

# Data Breach Exercise

- Think of this as a "murder mystery dinner"
- You will be divided up into a number of groups
- 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

# 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, victims, other state agencies, the media, and the public.

*During the event, you may be asked craft mock press release messaging about the scenario. Be prepared to respond to members of the media about what is happening and how your organization is responding.*

# District Data Breach Exercise (cont.)

**2. Response Plan** – Outline how the university 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

- You are employed by the fictional State of Confusion Higher Education Agency
- Your agency's information systems make use of State infrastructure and data centers
- Your State has recently faced increased pressure to strengthen its cybersecurity posture in the wake of several high profile data breaches

# Background and Scenario *(cont.)*

- To that end, the State is sending auditors to each tenant system to evaluate their security policies and controls. You are currently being audited.
- There is a team of State security assessors who are conducting interviews and going over logs and policies
- Your leadership team receives an urgent email from your IT Director to convene a meeting immediately.

# Emergency

- The auditors found evidence of a potential data breach in the logs they were reviewing. They immediately ceased their assessment.
- The events in question occurred 7 months ago
- Account logon events happened on days and at times when no employees were present
- State boundary security logs show what appear to be large data transfers happening on weekends and during the night
- The events appear to involve one particular employee, Stanley Smith, who is an application developer in the Dev shop

# Okay, What Now?

1. Gather with your team.
2. Go over the background and scenario carefully. What do you know? What don't you know?
3. Begin considering your approach to a response. Elect a team member to take notes.
4. We will regroup in 10 minutes. Be prepared to report how you plan on responding

- Questions?

# Questions to consider…

- Is this an actual breach?
- What should you do during this critical initial response?
- What, if anything, do you report? To who?

## *Data Breach Exercise*

# 10 Minutes

# Time to Regroup!

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

The State IT security folks have evidence that only one computer in the organization seems to be involved. Unfortunately it is the Dev source code repository that has a large test data set containing the PII of some 40,000 students. The amount of data transfers indicates that the entirety of the repository may have been exfiltrated.

# Scenario Update (cont.)

- You are unable to access detailed logs because the machine in question does not maintain logs more than 30 days.
- Stan Smith says he does not remember being at work during the times of the transfers
- He confirms that the test data set does contain PII but that it does not contain SSNs and that some of the details would have been swapped or muddled to test the matching engine.

# Scenario Update

- How does this change your response?
- What will you do in the next phase of the response?
- What information do you plan to provide?
- What are the assumptions you are making about the situation?
- Are you working on your resume?

## *Data Breach Exercise*

# 10 Minutes

# Time to Regroup!

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

# Scenario Update

- Further investigation indicates that the IP address to which the data was sent is a Comcast Cable residential IP address in the local area.
- The plot thickens as this IP address appears to be Mr. Smith's home residence.

# Scenario Update (cont.)

- Further interviews with Mr. Smith reveal that he was working on some development work during that time and remembered that he at one time had set up an automated script to update his home repository with the latest code so that he could continue to work at home
- This was not authorized by organizational leadership, and his supervisor was not aware.
- Mr. Smith thought he was helping to ensure the project was completed on time, and his home server was wiped after the project was completed.

# Questions to Consider…

- Was this a data breach?
- Do you notify the affected students?
- What actions do you take internally? What about Stan?
- What could the organization do to improve in the wake of this?

## *Data Breach Exercise*

# 10 Minutes

# Time to Regroup!

Let's discuss each group's response and how it may have changed due to new events.

# Wrap-up Excercise

- What did we learn about breach response?
- Does your organization have the policies and plans it needs to respond if a breach happens?
- How can organizations adapt their response to the evolutionary nature of breaches to ensure better, more accurate response?
- How could this exercise be more useful to you?

# 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