Data Breach Awareness Exercise

Wisconsin Association of Student Financial Aid Administrators

April 11th-13th, 2018

Sean Cottrell
Baron Rodriguez
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.
- Each group should assign 1 person as secretary, and 1 person as spokesperson.
- 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

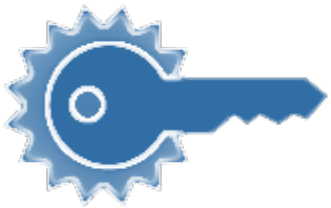
- Think about each of the roles needed in your organization (e.g., public information officer, data system leadership, attorney, auditors, etc.).

- 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.

University 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 to 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 Port Foozle University
- Port Foozle University is a large State school that is a major center of excellence for health and social research
- Over the last 15 years the university has been involved in wide ranging research on a variety of subjects using data gathered from schools, health organizations, and state agencies.

Background and Scenario *(cont.)*

- You receive word that an offsite storage facility leased by the research department has been the victim of a burglary over the weekend
- The facility was formerly used for storage of off-site backups, but is now simply used as a storage location for excess hardware and miscellaneous equipment
- It appears that several servers and a lockbox were stolen from the unit

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 to consider…

- Is this a data breach?
- What are the important things to understand about this situation to determine how to respond?
- 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 servers that were stored in the facility did not contain hard drives, however a few of the excess multi-function devices may have still contained drums or residual information like address books.

Scenario Update (cont.)

- The lock box turns out to be a small safe, which is locked.
- Unfortunately, the lock box appears to contain old backup hard drives containing research data
- The majority of the data appears to be encrypted, however there is a degree of uncertainty about what data is on the disks

Scenario Update

- How does this information change your response?
- What are the key next steps you will make to move the response efforts forward?
- Do you notify law enforcement? Who makes that call?
- Does the fact that a majority of the data was encrypted matter?
- 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

- You reach out to the researchers responsible and determine that the safe was put in storage because the research project was completed.
- The data set which was potentially backed up on the drives within the safe contains sensitive PII (including SSNs in some cases) for nearly 600,000 individuals.
- Researchers claim that most of the drive backups "should" be encrypted, with the exception of one database machine which did not have facilities for encryption.
- No one has a complete list of individuals whose data was on the drives, but the researchers do have a list of data sources.

Scenario Update (cont.)

- News of the break-in and theft has leaked to the media. Reporters are contacting the university asking for comment.
- Concerned potential victims, students, and State officials are making inquiries as to who was affected and what information was leaked
- The Governor's office is calling, demanding to know what the school is doing to remedy this situation

Questions to Consider…

- Was this a data breach if it was encrypted?
- Will you address the media? If so, what is the message you deliver?
- Do you notify the affected students? How?
- What actions do you take internally?
- Do you provide information to the governor's office about the response? To what degree do you share internal investigation data?

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 Exercise

- Let's hear your plans!
- What alternate paths did you consider?
- What should the school do in the wake of the incident?

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