Postsecondary ApplicationData Breach Scenario:
Facilitator’s Guide

Overview of the Exercise

This Data Breach Scenario is an interactive exercise designed to provide participants with the opportunity to experience firsthand the process and pitfalls of responding to a data breach at the organization level. Over the course of one to two hours, participants explore the scenario of a data breach containing student information as well as other personally identifiable information (PII) from their organization. Teams of five to seven people are asked to work together to define two important products:

* **Public and Internal Communications / Messaging**. *Develop the message you would deliver to your staff, students, parents, the media, and the public.*
* **Response Plan**, *Outline your agency's approach to the scenario and what resources you would mobilize. Describe the composition of your ideal response team and identify goals and a timeline for response activities.*

The facilitator should customize the scenario to the school district undertaking the exercise. The {bracketed phrases} in the text below indicate areas that you can easily customize for your district.

The Training Scenario

The training scenario revolves around the use of an {enterprise application} in a post-secondary institution. This application provides a platform for content and document creation, use, and management across the organization for both students and staff. This application is at the heart of how the school manages documents. Application administrators recently applied an update to the application which addressed certain issues relating to permissions and searching for content within the application. The update silently reset permissions on files affected by the update to a default “world readable” state. Some of the affected documents contain sensitive data like social security numbers (SSNs), names, addresses, and financial data.

The scenario will be rolled out in approximately 10-minute phases. After the initial scenario information is revealed, the teams will have 10 minutes to work. At the conclusion of each 10-minute segment, the facilitator will stop and review what has occurred, ask questions, and discuss what the teams have planned so far. Then, the facilitator will reveal additional scenario information. The facilitator should help the teams as they work by clarifying the scenario, prompting participants to consider all possible factors, and helping them to develop and frame questions.

Scenario Updates

After each of the first three work periods (10-minute segments) is complete, the facilitator will provide updates to the scenario, revealing more details of the breach, some of which might complicate the planned breach response. The purpose of introducing additional information is to illustrate that it is important not to jump to conclusions. In real life, we don’t have all information up front, and following a course of proper investigation reduce embarrassing mistakes. After each update, the next 10-minute timer is started. This process repeats until the workshop is completed.

Press Conference

During the fourth working period, the teams will prepare a press release. At this time, the knowledge of the breach has spread to the community, and the organization must respond. The teams will deliver their public message about the breach following this period. The public message should provide information and reassure the public. During this time, facilitators and other participants should listen carefully and ask questions about the breach and the message that is presented.

After each team has presented, discuss the successes and challenges of developing the public message.

The Response

The final period is spent developing and sharing Incident Response Plans, using the notes and processes developed as each team researched the breach and crafted its public response. While the point of the exercise is not to develop a formal Incident Response Plan, teams should address how the organization will

* identify an incident response team, including who is included in the team (for example, CIO, Data Coordinator, IT Manager, legal counsel);
* outline steps needed to identify and contain the breach, catalog the data affected, and identify how the leakage occurred;
* decide whether or not to notify any victims, and if so, when;
* determine what legal requirements affect the response, and develop a plan to ensure compliance; and
* plan to implement corrective actions to ensure there is not a breach recurrence.

After the plans are presented, group discussion should address the planning process as well as data breaches generally.

Closing

The closing discussion might include what the participants have learned, how it might affect future behavior, and lessons learned from the exercise (what could be done differently or better next time).

Facilitator Guide: Timeline of Events

(total time 60+ minutes)

Introduction (2 minutes)

* Introductions for facilitators and staff.
* Explanation of the exercise and scenario.
* Recommendations to get the most out of the experience.
* Products overview (Messaging and Response Plans).

Scenario Setup (2 minutes)

* Background information
	+ The organization
	+ Application details
* Breach
	+ Student notifies IT by phone
	+ Access to files they shouldn’t have access to
	+ 65k files affected
* Some contain SSNs and other PII
	+ Rules
	+ Divide into teams of five to seven people
	+ Go over the scenario
	+ Start to develop a response
	+ Explain exercise structure
* Questions

Work Period 1 (10 minutes)

* Answer questions about the exercise and scenario.
* Encourage teams to avoid knee-jerk reactions.
* At the end of the 10-minute period, survey the teams to determine progress on the initial response plan, and how they are responding to the initial information.

Update #1 (2 minutes)

* *Update 1* in the Handouts file includes this update information.
* Newspaper story claims FAFSA data available through the website
* Shows redacted pictures of student aid forms
* Exposure affected documents going back to 2005
* Spend only a short amount of time answering questions (remember as in real life, the information won’t all come at once).

Work Period 2 (10 minutes)

* Help develop questions.
* Ask participants to consider the sensitivity of the data types and to examine whether they should alter their response plans.
* Ask participants to spend a short time discussing controls that could avoid this breach scenario.

Update #2 (2 minutes)

* *Update 2* in the Handouts file includes this update information.
* IT reports that a recent update meant to address bugs in the permissions system inadvertently reset the permissions for some files to the default “world readable” state.
* These files were searchable.
* Most of the accesses for these files were from internal IP addresses, but some were from outside the school.
* The Higher Education Commission has begun an audit of your organization’s data security program.

Work Period 3 (10 minutes)

* Help coordinate questions.
* Help clarify questions to uncover the scope of the breach.
* Prompt the teams to consider how they will address the issue and what messaging they will use if it becomes publicly known.

Press Conference Time (10+ minutes)

* *Press Conference Time* in the Handouts file includes this information.
* During this work period, teams will craft a message to be shared at a “press release” with the whole group.
* Other participants and facilitators can ask questions from the standpoint of concerned students or local reporters.
* At the conclusion of the presentations, discuss how well teams represented their stories. Consider collecting lessons learned from the discussion.

Press Release Work Period (10 minutes)

* Help coordinate questions.
* Help focus efforts on clear and concise messaging.
* Prompt the teams to consider the messaging they will use from the perspective of the public and how this messaging may or may not differ from internal messaging for employees

Develop Incident Response Plan (10+ minutes)

* *Develop Incident Response Plan* in the Handouts file includes this information.
* In the final work period activity, each team will create an Incident Response Plan by consolidating their notes and ideas from the previous work periods. While a complete plan isn’t needed, the plan should address how the organization will
	+ identify an incident response team, including who is included in the team and who is involved (for example, CIO, Data Coordinator, IT Manager, legal counsel);
	+ outline steps needed to identify and contain the breach, catalog the lost data, and identify how the leakage occurred;
	+ decide whether to notify potential victims (and at what point);
	+ determine what legal requirements exist and develop a plan to ensure compliance; and
	+ propose corrective actions to prevent a breach recurrence.
* Have participants share and discuss the response plans. Ask questions relating to the development of the plans and about incident response and data breaches in general.

Incident Response Plan Work Period (10 minutes)

* Help coordinate questions.
* Help teams sort out previous discussions and provide access to previous slides for clarification.

Wrap up

Spend some time talking about the lessons learned from the press conferences and the ideas presented in the incident response plans. Discuss how those might or might not work for your district. The discussion might also include what they learned in the training, how it might affect future behavior, and what could be done differently or better next time.