Password Data Breach Scenario:
Facilitator’s Guide

Overview of the Exercise

The *Password* 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 district level. Over the course of 1-2 hours, participants explore the scenario of a data breach containing student information as well as other personally identifiable information from their school district. Teams of 5-7 individuals are asked to work together to define two important products:

* **Public & Internal Communications / Messaging** –develop the message you would deliver to your staff, students, parents, the media, and the public.
* **Response Plan** – outline how your agency will approach 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.

It is suggested that the facilitator customize the scenario to the school district undertaking the exercise.

The Training Scenario

The training scenario revolves around a common mistake: failure to create strong passwords and protect them from compromise. A teacher has written down his login information to the new student information system on a sticky note and put it on his desk. While he is gone, a couple of students discover the note. They then use the teacher’s login to access the system after hours and change students’ grades. Additionally, since the teacher used the same password on other internal systems, the students were also able to access other systems with sensitive employee data, including Social Security numbers and other private information.

The scenario will be rolled out in approximately ten-minute-long phases. After the initial scenario information is revealed, the teams will have ten minutes to work. At the conclusion of each ten-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 is encouraged to help the teams as they work by clarifying the scenario, prompting participants to consider all the possible factors, and helping them to develop and frame questions.

Scenario Updates

After each of the first three work periods (ten-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 of the information upfront, so it is best to follow the course of proper investigation to avoid embarrassing mistakes. After each update, the next ten-minute timer is started. This process repeats until the workshop is completed.

Press Conference

During the fourth working period, the teams will plan a press conference. At this time the knowledge of the breach has spread to parents and the community, and the organization must respond. The teams will deliver their public message about the breach following this period, providing information and reassuring the public. During this time, facilitators and other participants role-play reporters and parents, asking questions about the breach and the message that is presented.

After the press conference, time should be spent discussing 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 (e.g., 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 involve law enforcement, 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/better next time).

Facilitator Guide: Timeline of Events

(total time 60+ minutes)

Introduction (2 minutes)

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

Scenario Setup (2 minutes)

* Background information
	+ The school district.
	+ Centralized IT services.
	+ New web-accessed Student Information System (SIS).
* Breach
	+ Teacher put password on sticky note.
	+ Grades were changed.
	+ Other systems also affected.
* Rules
	+ Divide into teams of 5-7.
	+ 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)

* Breach occurred through the school’s Wi-Fi network after hours.
* The breach extends to other data loss, which included more sensitive data like SSNs.
* Reports have surfaced about students offering to change additional grades for money, though names have not yet been revealed.
* Spend only a short amount of time answering questions (remember as in real life, the information won’t all come at once).
* *Update 1* in the Handouts file includes this update information.

Work Period 2 (10 minutes)

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

Update #2 (2 minutes)

* Two juniors admit to breaking into the network and systems, using a teacher’s log-in information from the sticky note.
* They also admit to accessing other school systems that included employee data.
* Spend only a short amount of time answering questions.
* *Update 2* in the Handouts file includes this update information.

Work Period 3 (10 minutes)

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

Update #3 (2 minutes)

* The breach scope extends to include {insert desired number of students} students and {insert desired number of employees} employees.
* Investigators discover that the data have been posted to Facebook and other social media sites.
* Students have spread the knowledge of the breach beyond the school.
* *Update 3* in the Handouts file includes this update information.

Press Conference Time (10+ minutes)

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

Develop Incident Response Plan (10+ minutes)

* 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 what individuals are involved (e.g., 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 or not to involve law enforcement (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.
* *Develop Incident Response Plan* in the Handouts file includes this information.

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/better next time.