Data Sharing Dual Enrollment Scenario:  
Facilitator’s Guide

Overview of the Exercise

This *Data Sharing Dual Enrollment Scenario* is an interactive exercise designed to provide participants with the opportunity to experience 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 malicious ransomware incident affecting student information and other personally identifiable information from their organization. Teams of five to seven people will work together to develop a **Response Plan**, an outline of how your agency would 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.

The facilitator should customize the scenario for the school district undertaking the exercise.

The Training Scenario

The training scenario revolves around a data sharing scenario between a school district and a post-secondary institution. In this scenario, dually enrolled students attend a local community college for credit, and the college provides the students’ transcripts and grade information back to the school district so that the students can receive credit. The district maintains a file transfer service that the community college uses to share student data from the college to the district. A dually enrolled student is involved in a cyber bullying incident centering on alleged poor performance in the advanced college mathematics courses she is taking. Evidence is uncovered that grades may have been altered and that the incident of bullying may be related to the grade change.

The scenario will be rolled out in 10-minute-long 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 is encouraged to help the teams as they work by clarifying the scenario, prompting participants to consider all the possible factors, and helping them 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 incident, some of which might complicate the planned response. Introducing additional information will illustrate the importance of not jumping to conclusions. In real life, we don’t have all the information up front, so it is best to follow the course of proper investigation to avoid embarrassing mistakes. After each update, the next 10-minute timer is started. This process repeats until the workshop is completed.

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 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 that 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
  + Details of the school district and the data sharing agreement in place for dually enrolled students
* Incident
  + Concerned parents notify the school district of bullying
  + They claim their daughter is being bullied by classmates from her college courses about a failing grade
  + District records indicate she failed her final exam in Calculus II at the college
  + The student claims she did not fail her final exam and the grade is wrong
* 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)

* The district’s file transfer server appears to be normal. Nothing is out of the ordinary.
* The site uses FTP and requires a valid username and password to access the service. Only certain limited users at the district and community college have access.
  + Note: File Transfer Protocol (FTP) does not encrypt or protect any data sent using the service)
* The professor at the college confirms that Daniella did not fail her course
* The calculus professor states that the grade she has marked down is correct and is unsure how the grade at the district became different from her gradebook
* John, who is the person at the community college who sends the transcripts back to the district, confirms that he sent the grades properly and on time
* 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 methods to regain access to the data
* Ask participants to spend a short time discussing controls that could avoid this scenario

Update #2 (2 minutes)

* The online bullying began the day after the second file was uploaded to the transfer server
* Two of the main perpetrators of the bullying are computer science majors who were also in her Calculus II class
* One of the two is a student worker helping the IT department
* Logs from the FTP 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

Work Period 3 (10 minutes)

* Help coordinate questions
* Urge the groups to connect known information. They should connect the bullying with the second access of the server and the replacement of the grade data with tampered data.
* Help 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)

* One of the bullies admits the entire thing was an attempt to get back at Daniella for being a better student than the two bullies
* The other bully performed a Man in the Middle (MitM) attack and was able to obtain John’s password
* They then used the coffee shop to log into the district server and replace Daniella’s grade

Discussion Period

* Spend some time reviewing the issues from the start of the scenario to now. Ask the groups to consider what the organizations would be doing right now and to what extent they would engage with one another to identify and potentially turn over the information to law enforcement.
* Question the groups about where the legal and regulatory responsibilities rest. Is this incident grounds for a violation of the Family Educational Rights and Privacy Act (FERPA)?
* Discuss whether the scenario rises to the level of a data breach?
* Talk about whether to involve the authorities and at what point.
* Walk through what you now know with state laws around data breach. Is this a data breach under state law? If so, what must you do to comply with its requirements?
* Ask the groups to identify lessons learned and consider what the school district or community college could have done to avoid the situation or prevent this sort of activity.

Develop Incident Response Plan (10+ minutes)

* During the final work period, 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 (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.

Unveil Your Response Plan (10+ minutes)

* Have participants share and discuss the response plans. Ask questions about plan development and about incident response in general.

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 organization. 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.