Privacy Technical Assistance Center
U.S. Department of Education
(855) 249-3072
privacyTA@ed.gov
https://studentprivacy.ed.gov

Data Breach Scenario Trainings

Introduction

The Data Breach Scenario Trainings are a series of packaged trainings developed by the Privacy Technical Assistance Center, designed to help educational organizations at all levels conduct internal staff development on data breaches. Each scenario has been developed into a training package, providing ready-to-use resources for the scenario leader(s) and participants.

The Scenario Trainings each consist of three parts:

- The **Facilitator's Guide** leads users through the exercise, providing an explanation of its purpose, an outline of the activities and expected outcomes at each step, and suggestions for discussions along the way.
- The **PowerPoint Presentation** is provided for the leader's use during the exercise, providing slides and talking points.
- The **Handouts** are notes to be provided to each team, updating changes to the scenario as it progresses. These notes are also found in the slides. The facilitator should decide whether both tools are needed and edit accordingly.

All three pieces of each package are designed to be customized for your district: the Facilitator's Guide notes sections to adjust for the education organization's unique characteristics; the PowerPoint file has spaces for the education organization's name and logo, as well as a presenter's page; and the Handouts include space for both district name and logo, as well as areas for community personalization.

Scenarios

Password Data Breach Scenario

The *Password Data Breach Scenario* revolves around a common mistake, the 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 also were able to access other systems with sensitive employee data, including Social Security numbers and other private information. The goal of the activity is to highlight for district management the need to properly plan for a data breach, and illustrate the processes, procedures, and skills needed to respond. The package has three parts:

- Facilitator's Guide
- PowerPoint Presentation
- Handouts

Malicious Software Infection Scenario

The *Malicious Software Infection Scenario* revolves around the inadvertent ransomware infection of an organization that hosts a statewide longitudinal data system (SLDS). Ransomware is a type of malicious software that, when it infects a system, encrypts the contents and data of the system, making the data inaccessible to the system owners. The software then demands payment, usually in Bitcoin or other cryptocurrency, in order to provide the victims with access to their data again. In this case, the attack begins with two employees whose desktop computers become infected when browsing the internet. The ransomware then spreads itself to other systems within the organization, eventually impacting production systems and servers containing student data and other sensitive data types. The package has three parts:

- Facilitator's Guide
- PowerPoint Presentation
- Handouts

Postsecondary Application Data Breach Scenario

The *Postsecondary Application Data Breach 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 that 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, names, addresses, and financial data. The package has three parts:

- Facilitator's Guide
- PowerPoint Presentation
- Handouts

Data Sharing Dual Enrollment Scenario

The *Data Sharing Dual Enrollment 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 package has three parts:

- Facilitator's Guide
- PowerPoint Presentation
- Handouts

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.