Malicious Software Infection Scenario:
Facilitator’s Guide

Overview of the Exercise

This Malicious Software Infection 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 organizational level. Over the course of one to two hours, participants explore the scenario of a malicious ransomware incident affecting 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 & Internal Communications and 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.*

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

The Training Scenario

The training 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 scenario will roll 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 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 (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. 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 the information upfront, 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.

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, providing information and reassuring 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, 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 would

* 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 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
* Incident
	+ Employee laptops infected
	+ Demands payment
	+ No PII on laptops
* 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)

*These update cards provided in the kit are intended to present unforeseen complications and additional information to provide the responders with more information to inform their decisions. Some of the information will be critical to understanding the nuance of the scenario. The presenter’s notes on the accompanying slides in the PowerPoint indicate the appropriate time to distribute these updates.*

* *Update 1* in the Handouts file includes this update information.
* The malicious software behaves like a worm, infecting systems surrounding the infected machine using a vulnerability in the operating system to gain access.
* There is a patch for the vulnerability that would prevent further spread of the infection. It was released two months ago but some machines in the organization have not received it.
* Additional computers are becoming infected through unknown vectors.
* Some of these machines are servers with no direct user activity.
* One of these machines is a legacy server with an unknown quantity of student PII contained within.

Work Period 2 (10 minutes)

* Assist in developing questions
* Ask participants to consider the possibilities in regaining access to the data.
* Ask participants to spend a short time discussing controls that could avoid this scenario

Update #2 (2 minutes)

*These update cards provided in the kit are intended to present unforeseen complications and additional information to provide the responders with more information to make decisions on. Some of the information will be critical to understanding the nuance of the scenario. The presenter’s notes on the accompanying slides in the PowerPoint indicate the appropriate time to distribute these updates.*

* Servers are getting infected
* Normal operations impacted
* Pay or not?

Work Period 3 (10 minutes)

* Help coordinate questions.
* Help clarify questions about recovery. Encourage participants to talk about ways to get access to the data from backups, partner organizations, law enforcement, or even by paying the ransom.
* Prompt the teams to consider the messaging they will use to address the issue if it becomes publicly known.

Update #3 (2 Minutes)

*These update cards provided in the kit are intended to present unforeseen complications and additional information to provide the responders with more information to inform their decisions. Some of the information will be critical to understanding the nuance of the scenario. The presenter’s notes on the accompanying slides in the PowerPoint indicate the appropriate time to distribute these updates.*

* The local paper runs a story about the ransomware attack referencing the organization by name.
* The article insinuates that the entire organization’s data are affected and that all the data are corrupted.
* Parents and local privacy groups are asking about the status of the incident and demand details.

Press Release Work Period (10 minutes)

* Introduce the Press Release Development Exercise.
* Highlight the goals of the exercise and define expectations.
* Answer any questions about the exercise.
* 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.

Press Conference Time (10+ minutes)

* 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, 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 who is involved (for example, CIO, Data Coordinator, IT Manager, legal counsel);
	+ outline the steps to identify the source of the infection and curtail the spread, catalog the data affected, and identify how it occurred;
	+ determine what legal requirements exist and develop a plan to ensure compliance; and
	+ propose corrective actions to prevent a recurrence.

Unveil Your Response Plan (10+ minutes)

* Have participants share and discuss the response plans. Ask questions relating to the development of the plans and about incident response 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 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.