MISecure Data Theft Tabletop Exercise Facilitator's Guide

Introduction

MISecure has developed cybersecurity tabletop exercises to help districts prepare, practice, and rehearse your incident response capabilities. Go to the misecure.org website to view the collection.

About Data Theft Scenario

a. Purpose: This 1 hour scenario provides a district's executive team the opportunity to walk through a cyber incident as a team, testing their ability to evaluate business risk, coordinate response, and evaluate incident response plans.
b. Participants: District Executive Team, IT Leadership, Line of Business Directors (optional). Executive Team member or members are the key participant(s) in this scenario.
c. Prerequisites: No specific prerequisites although familiarity of the district's cyber incident response will better prepare the team for the exercise.
d. Expected Outcomes:
    i. Better understanding of the executive team's ability to respond to a cyber incident.
    ii. Improve ability to coordinate a response to an actual incident.
    iii. Improve the district's cyber incident response plan.
e. Length: 1 hour. Optional slides/injects are identified in the exercise which can extend the exercise if more time is available.
f. Scenario Theme: Data theft and extortion
g. Incident Severity: High
h. Facilitator: Experienced Facilitator

Running a Tabletop Exercise

Venue

- A conference room large enough to seat all participants with a comfortable seating arrangement conducive to discussion.
- Projector/screen for scenario presentation.

Materials

- None required although flip charts, markers, sticky notes, and whiteboard with markers/erasers can come in handy.

Pre-Exercise Communications

- Invitation Email Draft:

  Sent by Tech Director or Business Manager to their colleagues:
  Greetings District Executive Team,
  As you know, our IT team has worked with (name other teams) to develop a Cyber Security Incident Response Plan. This plan guides our district's response to cybersecurity incidents of different severity. We are inviting you to participate in a cybersecurity tabletop exercise to test our plan and provide an opportunity for us to work through a scenario together. This exercise focuses on the district's executive team's responsibilities during a cyber incident. During the exercise, you will evaluate business risk, coordinate a simulated response, and evaluate incident response plans. This is not a technical exercise. The exercise will last 1 hour and focus on the executive leadership role during a simulated cybersecurity incident. To prepare, we encourage you to become familiar with your district's cyber incident response plan. (LINK)
- Calendar Event with venue and timing information. Confirmation of attendance along with information about.

Facilitator's Role

As the facilitator of a tabletop exercise, your role is to

- Introduce the exercise and purpose
- Share Injects as presented in the slides and answer any clarification questions.
- Guide Discussion - focus on the purpose and expected outcomes for this specific exercise. The facilitator's primary role is to guide discussions, not to lead or dictate solutions. In this case, you want the focus to be on the executive level discussion.
- Let the team talk - if they are talking about cybersecurity you are winning.
- Timekeeping - mind the clock so that all topics can be explored.
- Help Participants Avoid Rabbit Holes - in guiding discussion, you may have to make up an answer to help focus the team get over a hump of the unknown. Be assertive when needed.

Participants for this Exercise

1. This is a small group exercise. The **district executive team** are the star participants in this exercise. More than one from leadership positions is desirable, but the exercise can be successful with one leader who has district wide authority to make decisions during an incident. This could be a superintendent or a deputy superintendent, or business manager, but the higher up the better.
2. **IT leadership** is there to play the role that they would play interacting with the executive leadership during an incident. They are not there to help provide context to what the scenario might mean to the district. The team works together to respond to business and/or financial impacts to the district.

3. Line of business leadership are welcome to participate, especially for those who have responsibility for sensitive financial data.
4. IT managers or staff can participate, but should consider their role more like observers - possibly answering questions if asked.

The Exercise

Each of the slides has talking points that go along with the slide content. Use that as a guide for highlighting key points.

Outline

- Introductions - have participants introduce themselves by describing their
- role during a cybersecurity incident.
  5 Minutes
- Overview Slides - A tabletop exercise is designed to have participants walk through a scenario together to test their planning and preparedness and rehearse a response to a realistic scenario. The scenario is realistic, but not real - assume that everything that is revealed happened. Active participation is required - participate as you would in an incident. The goal is to test and improve your resiliency, not individual capabilities. It is a learning atmosphere - focus on doing well, paying attention, and seeking opportunities for improvement.
  10 Minutes
- Scenario - the scenario is broken down into 4 sections. With 40 minutes, you can spend up to 10 minutes per section. Introduce each section or inject clearly and answer any questions that arise. Be as specific as possible. If you have to make up an answer to keep the team focused, you can do it - you are the dungeon master!
  Keep the discussion focused on the district wide risk perspective - they should be exploring the risks with information at hand.
    - Day 1: 6:00 AM: Data Theft Ransom Email - the HR director gets a threatening email.
    - Day 1 - 11 AM: Board President Reports Ransom Email - the same email that the HR director got.
    - Day 2: 10:00 AM: Call from the FBI - indications that a known threat actor is behind the incident.
    - Day 3: 5:00 PM: Quiet Incident Goes Public - local media asks for comment. This section is optional based on timing.

Hot Wash/Follow Up

- This exercise is designed to allow participants to identify lessons learned and follow up action items. The hot wash is a chance to have participants say some of these things out loud. Save at least 5 minutes for lessons learned and next steps. Encourage the team to document those and set up time for follow up. Look for specific updates to planning, including roles and responsibilities.

End and Thank You

End promptly to respect the time that the participants have offered.

Feedback on Exercise Content

Your feedback on the exercise can help improve the content for future exercise facilitators. Please share your thoughts with the MISecure Team https://misecure.org/contact/

Data Theft Exercise Details

Overview - purpose of exercise
Module Overview -
Module 1 - HR Director gets data theft ransom emailBrief narrative
Module 2 - School Board Pres gets ransom email
Module 3 - FBI confirms
Module 4 - Local news asks what’s going on