Disaster Recovery Tabletop Exercise Plan

A HEISC Resource

Participant Briefing Document

August 3, 2016
Introduction
The primary objective of today’s tabletop exercise is to explore some of the issues that will arise during an IT disaster scenario, some technical, some mission related. As our time during today’s online event is limited, this exercise has been deliberately crafted to run in a highly abbreviated time frame. You will receive a full tabletop exercise that you can conduct at your institution following today’s event.

Structure
This will be a facilitated tabletop exercise (TTX). Players will participate in the following modules:

- Module 1: Incident + Initial Response (30 minutes)
- Module 2: Secondary Impact (10 minutes)
- Module 3: Tertiary Impact (10 minutes)

Each module begins with an update that summarizes the key events occurring within a specific time period. Following the updates, participants review the situation and engage in brief discussion of appropriate response issues.

This document (“plan”) provides a written scenario and situation updates. Following each module is a series of questions that highlight issues for consideration during today’s exercise.

Ground Rules
- This exercise is deliberately shortened and designed to run in the time available today. You will receive a full tabletop exercise that you can conduct at your institution following today’s event.
- Work within the constraints stated by the scenario. Fight the problems, not the scenario.
- Respect the speaker.
- Enough, Let’s Move On (ELMO) will be used to keep the group moving forward and avoid becoming entrenched in the minutiae.
- All participants will receive the same information at the same time.

University Information
You are an employee of Michelynn University, a small, private, doctoral institution located in the Northeastern United States. Michelynn University has a liberal arts focus and a full-time enrollment of 10,000 students. It is consistently ranked in the top 30 national universities by U.S.
News and World Report and takes pride in its positive local and national reputation among current students and alumni. The learning management system is called Attain. The IT organization is called Information Technology at Michelynn University (ITMU).

**Scope**

The scope of this exercise should be strictly limited to the IT systems identified in the scenario. Do not spend time discussing how to recover from additional systems that would (in a real event) also be disabled by the simulated incident. Aspects of the exercise are necessarily contrived; some suspension of belief is required.

The following services are affected (i.e., “in play”) for today’s exercise:

- Attain
- Corn Administrative Hall and Tippens Data Center
- Michelynn University phone system
- Michelynn University primary website

The following services are unaffected (i.e., “out of play”) for today’s exercise:

- DNS
- Internet connectivity
- Other systems running on the virtualized infrastructure

**Role Play**

Feel free to ask questions based on the role that you actually have at your institution. Alternatively, you could take on one of these roles during the exercise:

- University president
- University CIO
- University CISO
- Information security analyst
- Policy chief
- University chief communications officer
- Building deputy
- Help desk manager
- Disgruntled ex-employee
- Concerned faculty member
- Concerned student
- Concerned parent
Module 1: Incident and Initial Response (30 minutes)

Incident: Wednesday, August 3, 2016, at 3:00 a.m.

Event 1: 3:00 a.m., August 3
At 3:00 a.m., a disgruntled ex-employee entered Corn Administrative Hall. She was terminated on July 29. However, her card access to university buildings had not yet been terminated, so she was able to enter the building and all ITMU communications rooms and data centers.

Once in the building she took a crow bar and smashed the Cisco ACE 30 load balancer, impacting Attain services. She then pulled the alarm bar and turned off building power (by pressing the circuit disconnect in a utility closet).

Event 2: 3:15 a.m., August 3
Michelynn University police arrive and, seeing the smashed equipment, quickly disable the alarm and declare the data center a crime scene. The police do not allow anyone to touch the core power switch for the building until a fingerprint expert arrives and tests the switch for fingerprints.

Event 3: 5:00 a.m., August 3
After hiding in the Vogel Library for a couple of hours, the ex-employee makes her way to the Tippens Data Center and physically removes the Cisco ACE 30 there. She then smashes the load balancer against the floor and leaves it there in pieces. The load balancer was also the front end to the campus authentication system, preventing authentication to the campus’s cloud backup instance for Attain.

Inject 1, 9:00 a.m. The ITMU help desk opens to a queue of 100 messages from students reporting that they are unable to log in to Attain. The help desk also receives 30 similar messages from faculty who have early-morning classes and are unable to access Attain.

Inject 2, 9:45 a.m. Social media is describing some sort of event requiring law enforcement on campus and the first calls from worried parents are starting to come in. The main Michelynn website (www.Michelynn.edu) is seeing an increasing load.

Module 1: Discussion Questions

Group
- Based on the information presented, what are your top priorities at this time?
- Who will be coordinating between departments?
- What is the chain of command for institutionally scoped decisions?

Technology Services
- What coordination among departments is necessary at this point?
**Academic Units**

- What procedures or communications might you undertake once learning about the incident?

*For the purposes of today's exercise, no discussion questions are asked for the following areas. A full tabletop exercise plan will be shared after today's event that includes questions for these areas:*

- University Services
- University Communications
- Public Safety
Module 2: Secondary Impact (10 minutes)

Inject 3, 10:00 a.m. Michelynn University police, working with local city police, have collected all the evidence they need from Corn Administrative Hall and allow ITMU staff to reenter and enable power to the building.

Inject 4, 10:15 a.m. The volume of calls to the help desk and to the general Michelynn operator are so large that general phone service is starting to fail—callers are getting busy signals and in general the phones are of intermittent use, even on campus.

Inject 5, 10:45 a.m. Using CCTV footage and in consultation with HR, Michelynn University police were able to identify the suspect in the incident under discussion and are working with area law enforcement to apprehend her. She is not believed to be on campus at this time. The individual is an ex-ITMU employee who was terminated for cause the previous Friday. The suspect had privileged access to all ITMU facilities and professional knowledge of the Michelynn computing environment.

Module 2: Discussion Questions

Group
- Based on the information presented, what are your top priorities at this time?

Academic Units
- What internal processes or communications with your faculty or students would you be implementing?

For the purposes of today’s exercise, no discussion questions are asked for the following areas. A full tabletop exercise plan will be shared after today’s event that includes questions for these areas:

- University Services
- Technology Services
- University Communications
- Public Safety
Module 3: Tertiary Impact (10 minutes)

Inject 6, 11:00 a.m. A Facebook posting claims that a bomb went off on the Michelynn University campus and that’s why no one can get through on the phone. Michelynn Public Safety officials are certain that there is no credible campus bomb threat. The Michelynn home page receives hundreds of times its normal load and becomes unresponsive.

Module 3: Discussion Questions

Group
  • Based on the information presented, what are your top priorities at this time?

Technology Services
  • What is the priority of repair or restoration of systems?

Academic Units
  • What is your role in responding to inquiries from parents or alumni?

For the purposes of today’s exercise, no discussion questions are asked for the following areas. A full tabletop exercise plan will be shared after today’s event that includes questions for these areas:
  • University Services
  • University Communications
  • Public Safety