

Sharing a Proven Tabletop Exercise Format and Scenarios

Scott Mulert, Ameriprise Financial

Agenda

- Introduction
- A proven format
- Development approach
- Three scenarios
- Examples of content
- Tailoring the scenario
- Facilitation approach
- Q & A

Exercise Format

- Introduction
 - Objectives
 - Ground rules
- Three panel scene detail
 - Scenario updates
 - Questions to consider
 - Items to review
- Discussion/Wrap-up
 - Lessons Learned
 - Action Items

Scenario Development

- Generate ideas from
 - Actual events
 - Media stories
 - Near misses
 - Plausible daydreams
- Draft and edit
 - Keep it simple... not always necessary to say “why?”
 - Personalize it for the situation
 - Make it plausible
- Review and modify
 - Engage targeted business partners
 - Engage targeted technical experts

Scenario – Water Damage

A Monday in October

- **6:30 AM:** Employees arriving to work have reported standing water on three floors of your office building.
- **7:00 AM:** Facilities management has confirmed water damage to the three floors and one additional floor.

Later that morning

- **9:00 AM:** Affected employees continue to arrive.
- **10:30 AM:** Facilities reports the source is a water cooler on the uppermost floor that was leaking heavily through the weekend. Facilities has confirmed that at least parts of the four floors are unsuitable for habitation and employees will be displaced. The duration will depend on the extent of the damages.

Later that day

- **3:30 PM:** Facilities has engaged a reclamation vendor that is attempting to clean and dry the area, but has no estimates on when the floors will be reopened.

Thursday morning – two days later

- **8:00 AM:** Facilities reports that although efforts to dry carpets and other flooring have been largely successful, mold has been detected. Full testing will need to be conducted, but it appears that flooring will have to be removed and replaced. It is unknown how long the floors will be uninhabitable.

Friday afternoon

- **1:00 PM:** Mold testing confirms that flooring will have to be replaced. Facilities is estimating that some employees may be able to return within one week if all goes well.

The next week – Tuesday

- **8:00 AM:** Work to remove flooring is complete, but the installation of new flooring is delayed to allow the concrete to dry. It could be up to 28 days to get the concrete completely dry, prior to new flooring installation.

Six weeks later

- **5:00 AM:** The floors have re-opened to all employees.

Scenario – Severed cables

A Tuesday afternoon in June

- **1:40 PM:** Offshore employees in India have lost all network connectivity. Technology is working to identify the issue.
- **1:50 PM:** A critical vendor has also lost all network connectivity, and are unable to move data to you.
- **2:10 PM:** Technology has been working with their vendors to identify the issues, and has confirmed that the outages appear to be a telecommunications issue that is affecting many companies. There is no estimated resolution for the outages.

Later that day

- **4:30 PM:** Technology has received word that at least a few underwater cables have been severed. An additional non-critical vendor is impacted. Although the critical processes are architected with dual cables, it appears the telecommunications vendor bundled them together and both were severed. Prior cable accidents have taken up to a few days to repair.

Thursday - two days later

- **9:00 AM:** News reports are speculating that a foreign government may be intentionally severing undersea cables, most likely the Russians. Additional reports of severed cables were made yesterday and early morning. There do not appear to be any additional impacts to your processes.
- **10:00 AM:** The Telecommunications vendor is reporting they have not yet found where the cable is severed, and it may be in deep ocean waters. Estimates for repair are unknown.

Friday – the next day

- **7:00 AM:** The Telecommunications vendor has located where your impacted cable is severed, but they are reporting it may take an additional week to fix due to the location in the ocean.
- **8:00 AM:** News reports confirm no new cables have been cut, but widespread impacts persist across a number of sectors. Financial markets are reflecting the impacts, with stocks off substantially the last two days. No governments have claimed responsibility.

One week later

- **8:00 AM:** Your services have been restored, but other companies are still experiencing outages. Nobody has claimed responsibility, but officials believe the cables were intentionally severed.

Scenario – Team Lottery Win

Monday morning

- **9:00 AM:** An executive reports that an operational team has not shown up for work. Attempts to contact team members have failed; nobody from the team has answered their phones. Messages have been left, but none returned.
- Rumors are swirling that something may have happened to the team. Corporate Security has been contacted and has contacted public authorities.
- **9:30 AM:** The executive relates that there are three essential daily processes that only a few individuals on the team understand how to complete.

Later that Monday

- **11:00 AM:** Police visited the household of an employee and discovered a celebration happening. Most of the team members were present. The officer prompted one team member to call the executive and confirm that the entire team was in a workplace lottery pool that hit a 900 million dollar jackpot that weekend.
- The executive was informed that the entire team had calculated that they didn't need to work again, and had not yet decided whether they would ever return – but definitely not today.
- **3:00 PM:** The executive was able to reach one former team member that is still with the company, but is on vacation. The employee was reached by phone and was able to talk someone through the most critical and basic part of the business processes. Other parts of the process are being delayed until the next day.

Tuesday morning

- **9:00 AM:** Human Resources has been engaged to attempt to negotiate a short-term contract with the lottery winning team to return and complete training. There has still been no response.
- Additional measures are being made to work remotely with the former team member on vacation.

Wednesday afternoon

- **1:00 PM:** Negotiations with the lottery winning team has resulted in a limited return of two resources to train others. Hiring replacements is being prioritized.

Questions To Consider - Examples

- What is the process for communicating a facility outage (after hours)?
- During business hours, how do we account for all personnel?
- How are leaders staying in communication to coordinate response? What is the updates' frequency?
- Which critical business functions can be handled by another office? Who is responsible for notifying them and what information needs to be shared?
- How many employees are configured to work from home? When was the last time they did so?
- What information should be given to employees? Who makes this decision and who communicates it?
- Who makes the decision about using an alternate work location for the next day? How will this information be communicated?
- What dependencies exist on other business groups? What will you do if they are also impacted?

Questions To Consider – Examples cont.

- What is the process for communicating a systems outage?
- How and when are issues escalated to department leadership?
- What are the most important considerations at this time?
- Who else needs to be made aware of the problem?
- What additional actions should you be considering?
- How is communication flowing between your department and Technology?
- What information will be shared with key business partners, vendor partners and customers? When will it be shared? How will these notifications be handled?
- How long can your department tolerate a systems outage? How long will your manual procedures keep your critical processes adequately functioning?

Items To Review - Examples

- Review plan roles to ensure accuracy and understand responsibilities.
- Who are your Crisis Team representatives?
- Review your business continuity plan's contact information to ensure it identifies all critical business partners, vendor partners and customers. Ensure that the contact information is current.
- According to your BCP, which positions support which critical business processes and at what time frames? When was the last time these positions / roles were reviewed? Review and update, as required.
- What does your BCP say about work-from-home capabilities? What work-from-home procedures are documented in the plan?
- What does your plan say about transferring work to another operating location or outsourcing to a vendor partner?
- Are there any items, other than standard office supplies, that your group requires to continue critical processing without access to the facility?

Items To Review – Examples cont.

- When does your BCP say updates will be given to key business partners, vendor partners and customers? Who does it say will make these updates and how are they to communicate the information?
- What does it say about procedures and mechanisms to prioritize work and continue operations in a work-from-home or alternate location?
- According to the plan, how does communication flow to personnel working from home or at an alternate facility?
- According to the plan, how often, and to whom, are status updates given?
- According to your plan, which employees support critical business functions? When was the last time the list was updated? When was the last time these employees reviewed or tested manual procedures?
- What does your plan say about transferring work to another operating location or outsourcing it to a vendor?
- Who does your plan say will make the decisions about moving to alternate work locations and/or dismissing employees for the remainder of the day? How does your plan say this information will be communicated?

Tailoring the Scenario

- Alter the duration
- Remove their solution
- Compound the problem
 - Add another location
 - Add another crisis
- Make it less complex

Approach to Facilitation

- Use an agenda
 - Published
 - Hidden
- First priority is to ensure delivery of the business objectives
- Maintain control
- Allow for discussion to wander
- What gets documented gets done

Q&A

Questions?