A scenario is a simple outline of a plausible sequence of fictional events that provides the backdrop for participant discussion during the exercise. The scenario needs to be realistic and challenging, but not so complicated that it overwhelms participants. When creating a scenario, keep the following in mind:

> **Keep It Real**
Think about the issues, threats, and hazards that face your business and your community. The situation should be informed by the risks you face. For example, if you are in an earthquake-prone area, the scenario could feature a high-magnitude, high-intensity quake. If your business is located near railroad tracks used by freight trains, you could create a scenario that involves the derailment of a train carrying toxic chemicals. On the other hand, if you live in the Upper Midwest, a hurricane is not the best choice, just as a major snowstorm would not be realistic for southern Florida.

> **Make Sure the Scenario Supports Your Objectives**
When identifying or developing a scenario, choose an event that best supports the objectives you want to achieve in the exercise. If you want to test protective security measures, then consider a scenario involving a malicious infiltration or possible terrorist attack on your facility. If you want to test technology issues, then develop a scenario that will stress your networks or cyber infrastructure, such as a cyber attack or a sustained power loss. If you want to validate personnel evacuation procedures, then develop a scenario such as a fire or explosion that tests how you move people out of your facility.

> **Think About Day and Time**
The date and time specified for the scenario event will affect the issues discussed as part of the exercise. Think about how the population in your business and your community as a whole changes on weekdays, weekends, and holidays, as well as at night and during special events.

> **Consider Different Event Phases**
You can divide the scenario into segments or chapters to help manage the flow of the exercise and make it easier for participants to work through issues that occur at different points in an event timeline. For example, if the scenario involved an explosion, you could consider issues that might arise pre-incident when a threat is detected, within the first hour of an incident occurring, within the first 12 hours, and after the first 12 hours.
Using Scenarios in Tabletop Exercises

> Consider Multiple Events through Short Vignettes
Rather than using one lengthy, complex scenario, you may want to consider using several vignettes that are shorter and less detailed. Vignettes allow you to explore a set of discussion questions within the context of different situations. This approach could be especially valuable if you do not plan to conduct more than one exercise in the near future or if you are concerned about multiple hazards.

Example Scenarios

1. Train Carrying Toxic Chemicals Derails
2. Flu Pandemic Threat
3. Cyber Attack is Launched
4. Rainstorms and High Winds
5. Detonation of Explosives
Example #1

Train Carrying Toxic Chemicals Derails

Pre-incident:

A major freight railroad line traverses your region, carrying critical commodities such as chemicals, grain and other agricultural products, coal, steel, minerals, and motor vehicles and motor vehicle parts.

Incident:

At 10 a.m. on a weekday, a 50-car train carrying toxic chemicals derails two miles from your business. A dozen tank cars jump the track and begin to release their contents. A major fire spreads across the train, releasing smoke and potentially dangerous fumes. Emergency responders arrive quickly to the scene, evaluate the potential threat of a major explosion or a dangerous vapor release, and determine the cause of the derailment.

Post-incident:

Within one hour, emergency managers call for a mandatory evacuation of residents and businesses in a one-mile radius because of dangerous fumes emanating from the train. The winds are relatively calm and your business is located upwind. However, weather officials expect the winds to shift and pick up intensity over the next 24 hours. Emergency management officials are not predicting the duration of the evacuation, although rumors abound that it could last up to a week. Within three hours of the derailment, approximately 20 people report to a local hospital with breathing difficulties and burning eyes.
Example #2

Flu Pandemic Threat

Pre-incident:
A new flu strain begins to emerge in the Caribbean, sickening and killing dozens of people who either live in the region or have traveled there as tourists. Public health officials are monitoring the situation and note that anyone who has visited the afflicted areas within the past month could be a possible carrier.

Incident:
Within one week, 10 people in your community are diagnosed with this particular strain of flu. Absentee rates at local schools begin to spike. Businesses across the region report that they are experiencing increased absenteeism as employees stay home to care for children, become sick themselves, or simply opt to shelter themselves at home voluntarily.

Post-incident:
Within three weeks, many businesses in the region report that as much as 40% of their workforce is absent, consequently straining critical operations.
Pre-incident:
Your network security team has detected a significant increase in attempted intrusions on your corporate network. Staff are reminded to change their passwords regularly and lock their workstations while away from their desks.

Incident:
A series of coordinated cyber attacks by an unknown party (or parties) is launched to disrupt components of the Nation’s information technology, energy, and transportation infrastructure. The attacks cause major Internet and telecommunications slowdowns that cripple even the simplest of transactions across large segments of the Nation. Electrical power generation ceases in a multi-state region in which your business is located.

Post-incident:
Public and private sector officials struggle to identify the attack source and get systems online. The power outages are expected to last for days and have major impacts on infrastructure sectors that rely heavily on the Internet. The attack has major implications on telecommunications and transportation, including air and rail, across the country.
Example #4

Rainstorms and High Winds

Pre-incident:
A major front approaches the area, threatening to bring heavy rain, thunderstorms, and high winds. Forecasters predict 6 inches of rainfall across the region within the first 24 hours, with as much as 9 inches in some locations.

Incident:
The heavy rains and wind arrive, snarling traffic as flood waters and debris block passage in a number of areas across the region. The slow-moving front lingers for almost four days. The 60-mph winds knock down dozens of trees, cutting nearby power lines and blocking roads entirely.

Post-incident:
Within 72 hours, more than 11 inches of rain fall, raising concerns about flash floods and mudslides. Local officials close roads in some nearby communities and evacuate residents and businesses located nearby. School systems cancel classes for two days to keep students safe and minimize driving throughout the area during the height of the storms. The wastewater treatment facilities in several communities are flooded, as are multiple sewage pumping stations. A major interstate highway is forced to close for 36 hours. Power outages are widely reported across the region because of trees and branches knocked down by the winds. Nearly 100,000 buildings suffer mostly minor damage because of water and wind.
Example #5

Detonation of Explosives

Pre-incident:
On a quiet weekday afternoon in January, an anonymous individual drives into a large local retail shopping center in a plain white van. The person stops the van in a no parking zone in front of the center's largest retail store and begins to take pictures of the building, including entry and exit points. The individual then moves the van to a legal parking spot, enters the store, and begins to take pictures inside, paying special attention to restricted access areas, security cameras, and entry and exit points.

Incident:
Several weeks later, at the height of the President's Day Weekend sales rush, two attackers arrive at the shopping center. They each carry backpacks filled with explosives and carry concealed semi-automatic weapons under their jackets. They walk into the largest retail store, separating as they enter and establishing positions at opposite sides of the facility. The backpacks are left unattended near the main entrances so that the exits will be blocked when the explosives are detonated. At a pre-determined time, they detonate the explosives hidden in the backpacks and begin firing their weapons.

Post-incident:
Panic and chaos ensue, with shoppers fleeing to the main entrance of the store in an attempt to evacuate the area. Dozens of people begin to gather in the parking lot awaiting instructions and medical care from emergency responders, who arrive within 10 minutes of the attack. Inside, two different groups of employees are able to tackle the shooters, knocking away their firearms and subduing them for 10 minutes until law enforcement arrives.