

**Business Continuity Toolkit Resource**

**Example Exercise Scenarios and Injects**

*The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.*

**Contents**

1. Introduction 2
2. Initial scenarios and related injects 2
3. Common facilitation injects 4
4. Introduction

This resource is part of the business continuity management (BCM) toolkit and it provides examples of scenarios and injects (developments) that can be used to conduct table-top exercises. These exercises help test the effectiveness of documented continuity plans and the knowledge of personnel responsible for response and recovery activities.

Table-top exercises are discussion-based simulations that rely on specific disruption scenarios and ‘injects’ that develop or escalate the situation. Time should be allowed for participants to react to the initial scenario and after each inject, and their response should be measured against the documented continuity plans.

These scenarios and injects are provided as examples and may not be relevant to all situations. Businesses may use this resource to obtain a better understanding of the available exercise scenarios to test their continuity plans.

1. Initial scenarios and related injects

Disruption scenarios can be any event that impacts critical resources, such as people or technology systems, and one scenario may impact multiple types of resources simultaneously.

The following list includes common disruption situations which could be used as the initial disruption scenario, as well as injects relevant to each scenario:

|  |  |
| --- | --- |
| **Initial scenario** | **Sample injects** |
| Critical production assets and some inventory has been stolen during peak demand season. | * A major customer learns about the theft and inquires if their order will still be fulfilled on time
* The media accuses an insider of orchestrating the equipment and inventory theft.
 |
| A labor strike is organized by production staff before fulfilling a major customer order. | * A major customer learns about the strike and inquires if their order will still be fulfilled on time
* The media publishes unconfirmed stories about unfair treatment of the production staff, justifying the strike.
 |
| A fire or explosion occurs which impacts the primary facility/office space and some personnel who were onsite at the time of the incident. | * The facility manager alerts management that a number of employees have been injured in the fire
* A service provider contacts a member of management inquiring about the status of their personnel that were onsite during the fire.
 |
| A key piece of equipment malfunctions during a time with low inventory stockpile. | * A new order comes in requesting a large amount of goods/services to be delivered in 2 weeks
* Management discovers that the primary vendor of the equipment and its spare parts has been facing financial challenges and has since filed for bankruptcy.
 |
| A prolonged utility outage occurs during business hours at customer-facing locations, which began while customers are in the facility. | * The outage occurred while customers are onsite and have already paid for their entry, and are now demanding refunds
* The facility manager informs management that the outage is expected to last for 2 days.
 |
| A key supplier/third party abruptly files for bankruptcy without advance warning of their financial challenges. | * The procurement supervisor informs management that this supplier was expected to fulfil a major delivery in 2 days, but will now be unable to deliver the supplies.
 |
| A natural disaster or severe weather situation occurred which prevents some staff from reaching work sites. | * HR notifies management that 50% of staff will be unable to reach the facility/office for the next 2 working days
* Some staff already onsite will be unable to leave the facility to reach their homes and require temporary accommodations.
 |
| Physical vandalism, natural disaster or severe weather occurs which damages a facility and the inventory contained within it. | * Supervisors inform management that 50% of the inventory on hand has been destroyed and the remainder is not sufficient to fulfil current customer orders
* Supervisors inform management that key production equipment has been partially damaged and requires repairs and spare parts, taking at least 5 days to recover.
 |
| A suspected cyber-attack has occurred which appears to impact critical system availability and laptops. Users begin to see a full-screen message saying their laptop is locked and asking for a bitcoin payment to unlock it and recover their data. | * IT personnel report that some of their server-hosted tools are not accessible
* Many calls are received by the helpdesk reporting this issue. The users support a variety of critical and non-critical processes
* The information security team handling the incident response informs management that more than 50% of laptops and servers for 3 critical applications have been impacted by the ransomware and the time to unlock them is unknown at this point
* The information security team informs management that a solution has been found to unlock the infected machines.
 |
| A cyber-attack compromises the confidentiality of customer data. Local police authorities contact a member of management to inform them that some confidential data has surfaced online that looks like it came from the organization. | * Customers contact the call center to inquire about the potential data breach and the security of their data
* The information security team informs management that the source of the breach has been identified and contained.
 |

Note: additional scenarios can be derived from the threats raised in the continuity risk assessment stage.

1. Common facilitation injects

The following list includes generic injects that can be used under multiple scenarios, which are intended to progress the exercise and to also test common responses to external stakeholders.

Facilitation injects to progress the exercise scenario:

1. The management team decides to declare a crisis/disaster and activate continuity plans
2. The initial damage assessment indicates that a specific resource will be unavailable for 2 weeks
3. Internal staff contact departmental management to ask when a particular resource will be available again
4. The management team requests updates from personnel in charge of emergency response or business process recovery
5. The business continuity coordinator communicates to all impacted personnel that the disruptive situation is over, and they can begin return-to-normal activities to resume the original mode of operations and wind-down temporary operations/measures.

Generic injects relevant to most scenarios:

1. Building security communicates to management the presence of a reporter asking for information about the incident
2. Local police authorities contact a member of management to request more information on the incident
3. Customers voice their concern on social media about the disruption and how the organization is handling it so far.