**Name** : **Rizqi Zamzami Jamil**

**Class** : **SIB-4C**

**NIM** : **2141762089**

# Lab - Recommend Disaster Recovery Measures

## Objectives

**Part 1: Natural DisasterPart 2: DDoS Attack Part 3: Loss of Data**

## Background / Scenario

Every organization needs to be prepared for a disaster. The ability to recover from a disaster can determinethe survival of the business. A disaster can be a hurricane or typhoon, hardware failure, loss of data, or a devastating cyber attack.

A disaster recovery plan will include policies and procedures that the organization follows when IT servicesare disrupted.

In the plan, you should take into account IT-related people, services and equipment, and the physical locations of the business. You should also keep in mind of recovery point objectives (RPO) and recoverytime objectives (RTO).

In this lab, you will recommend disaster recovery measures for a natural disaster, equipment failure in thedatacenter, a DDoS attack, or loss of data for a tutoring service.

In this business, you have students from different geographical locations who require tutoring for differentsubjects, such as mathematics and language. The students have access to an online curriculum that provides them with supplemental materials based on their needs. The students can also sign up for personal assistance from instructors for scheduled small group or one-to-one tutoring services. The business has a few physical locations that potential customers can visit and use the tutoring services in- person. The business delivers services to its customers from a neighboring cloud data center. The data center delivers instructional content, student records, registration for services, and real-time video conferencing for direct instruction. Other routing business practices, such as backups of onsite business servers is handled in the data center.

## Required Resources

- Device with internet access

## Instructions

### Part 1: Natural Disaster

A hurricane, or typhoon, has struck your community and caused damage near a data center. The networkinfrastructure in the area has also suffered damage.

The damage near the data center has caused a network outage and the servers in the data center are nolonger accessible remotely. Because of the extensive damage in the community, it may take a few days before a thorough damage assessment can be completed. You can assume that there is no access to thisdata center for at least a week.

### Step 1: Identify the potential risks.

Questions:

Answer the following questions:

Can the business operate without access to this data center? Explain.

**Answer:**
No, the business cannot fully operate as critical services like online curriculum and video conferencing are hosted in the data center.

Can the students access their online materials? Explain.

**Answer:**
No, students cannot access online materials since they are stored in the affected data center.

Are there other ways that instructors can provide the tutoring services? Explain.

**Answer:**
Yes, instructors can provide in-person tutoring at physical locations and use alternative video conferencing tools temporarily.

Can new users sign up for the tutoring services? Explain.

**Answer:**
No, since the registration system is hosted in the affected data center.

Can the employees access internal company information during the recovery?

**Answer:**
No, internal company information stored in the data center would be inaccessible.

## Step 2: Recommend a disaster recovery plan.

Based on your answers in the previous step, list your recommendations below:

**Answer:**
1. Implement redundant data centers in different geographic locations
2. Create offline backup copies of critical materials
3. Establish alternative communication channels
4. Set up emergency registration procedures
5. Deploy cloud-based backup systems

# Part 2: DDoS Attack

A few users have reported that they cannot log into their accounts and access the online curriculum. Upon further investigation, it appears that the web server is overwhelmed with requests at a time when normally there is little traffic. It appears that the server is undergoing a denial of service attack.

## Step 1: Identify potential problems.

questions:

Answer the following questions:

Can the business operate without access to data center? Explain.

> **Answer:**
> Partially, but core online services would be disrupted.

Can the business still function without access to the data center? Explain.

> **Answer:**
> Limited functionality would be possible through physical locations.

Can the students access their online materials? Explain.

> **Answer:**
> No, the DDoS attack prevents access to online resources.

Can the instructors still provide the tutoring services? Explain.

> **Answer:**
> Yes, but only through in-person sessions at physical locations.

Can new users sign up for the tutoring services? Explain.

> **Answer:**
> No, the registration system would be inaccessible during the attack.

Can the employees access internal company information during the recovery?

> **Answer:**
> Limited access depending on which systems are affected by the DDoS attack.

## Step 2: Recommend a recovery plan.

Based on your answers in the previous step, list your recommendations below:

> **Answer:**
> 1. Implement DDoS protection services
> 2. Set up traffic filtering
> 3. Deploy content delivery networks (CDN)
> 4. Establish backup communication channels
> 5. Create incident response procedures

# Part 3: Loss of Data

Users have reported that they are unable to login to their accounts, and they were unable to reset theircredentials. Other users have reported that they were able to log in, but their recent progress in their classes is missing. After further investigation, it appears that the data loss was caused by human error.

## Step 1: Identify potential problems.

questions:

Answer the following questions:

Can the business operate with the data loss? Explain.

**Answer:**
Partially, but with significant disruption to online services.

Can the students access their online materials? Explain.

**Answer:**
Yes, but their progress and personalized content may be lost.

Can the instructors still provide the tutoring services? Explain.

**Answer:**
Yes, but without access to student history and progress data.

Can new users sign up for the tutoring services? Explain.

**Answer:**
Yes, but the registration system needs to be restored first.

Can the employees access internal company information during the recovery?

**Answer:**
Limited access depending on what data was lost.

### Step 2: Recommend a recovery plan.

Based on your answers in the previous step, list your recommendations below:

**Answer:**
1. Restore from latest backup
2. Implement regular backup procedures
3. Create data recovery protocols
4. Establish data validation processes
5. Deploy automated backup systems

## Reflection

1. These cases indicate disaster recovery requirements that are common to many businesses that use offsitedatacenters. What should be included disaster recovery plans for many of these business?

**Answer:**
Essential elements for disaster recovery plans should include redundant systems, regular backups, alternative communication methods, and clear recovery procedures.

2. Now that you have examined a few scenarios and provided some possible disaster recovery measures,what other actionable recommendations are essential for a successful disaster recovery?

**Answer:**
Additional essential recommendations include regular disaster recovery testing, employee training, documentation updates, and establishing clear communication protocols during emergencies.