Name : Selly Amelia Putri

Class : SIB 4C

Lab - Recommend Disaster Recovery Measures

Objectives

Part 1: Natural Disaster

Part 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 determine the 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 services are 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 recovery time objectives (RTO).

In this lab, you will recommend disaster recovery measures for a natural disaster, equipment failure in the datacenter, 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 different subjects, 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 network infrastructure 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 no longer 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 this data center for at least a week.

Step 1: Identify the potential risks.

Answer the following questions:

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

No, the business cannot fully operate without access to this data center. While limited functions may continue at physical locations, the business's core operations depend on remote access to the data center. This dependency arises because:

- Customer Access: Customers rely on the data center for access to tutoring services and online content. Without this access, they cannot receive the services they paid for, potentially leading to customer dissatisfaction and revenue loss.
- Instructor Access: Instructors also depend on the data center to access essential student information and deliver tutoring sessions. The inability to retrieve or update student records could disrupt lesson continuity and affect instructional quality.

Consequently, without the data center's functionality, both customer-facing services and instructional operations are significantly impaired, making it difficult for the business to function effectively.

Answers will vary. The business will have limited functions at the physical locations only. The business requires access to the servers within the data center remotely. Without them, the business cannot function because the customers cannot access the tutoring services and the online content. Furthermore, the instructors cannot provide tutoring and cannot access the student information remotely.

Can the students access their online materials? Explain.

No, students will not be able to access their online materials if those materials are hosted solely within the affected data center. Since this data center is currently inaccessible, all content stored there remains unreachable, preventing students from accessing learning materials. This disruption could hinder their progress and satisfaction, especially if no alternative access options are available.

Answers will vary. The students will not be able to access the online materials if all the materials are located in the same inaccessible data center.

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

Yes, instructors can still provide tutoring services by connecting with students through alternative platforms, such as video conferencing applications provided by third-party services (e.g., Zoom, Microsoft Teams, Google Meet). Although instructors may lack access to specific resources stored in the data center (like detailed student records and materials), they can maintain communication and continue basic tutoring sessions. This temporary solution would allow tutoring to continue, though it may be limited in terms of access to personalized materials and session history.

Answers will vary. The instructors can still provide services if they can connect with students via meeting applications that are provided by other online providers.

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

No, new users cannot sign up for the tutoring services if the sign-up process and user database are managed within the inaccessible data center. Without access to this online database, the system cannot register new users, create accounts, or process enrollments. This limitation prevents the business from onboarding new clients, potentially impacting revenue and client acquisition until the data center is restored.

Answers will vary. New users cannot use the service if they cannot access the business's online user database that is housed in the inaccessible data center.

Can the employees access internal company information during the recovery?

No, employees cannot access internal company information if the internal servers, housing essential resources and data, are located within the same inaccessible data center. This lack of access could hinder

internal communication, project management, and administrative functions, making it challenging for employees to perform their roles fully during the recovery period.

Answers will vary. The employees cannot access internal information if the internal servers are also located at the same data center.

Step 2: Recommend a disaster recovery plan.

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

- Maintain an Up-to-Date Backup of Essential Data: Establish a secondary data center or cloud-based backup containing a current copy of the user database, online curriculum, and critical internal resources. This backup should be updated regularly to ensure the latest data is available for recovery.
- Establish a Secondary Location with a Different ISP: Set up a secondary physical data center in a geographically separate location with a different ISP, reducing vulnerability to region-specific outages and ensuring alternative connectivity options.
- Enable Rapid Activation of Backup Services: Configure the backup location to activate quickly in the event of primary data center inaccessibility, minimizing downtime and ensuring that users and employees can access essential services.
- Internal Server Access for Employees: Ensure employees can access a backup of internal servers that include updated information, internal documents, and necessary tools for operations during recovery.
- Distribute Local Copies of the Disaster Recovery Plan: Provide each employee with a local copy of the disaster recovery plan, detailing roles, contact points, and processes to follow during an emergency, ensuring preparedness and smooth execution of the recovery process.

Answers will vary. This business cannot function successfully without access its user database and online curriculum. A backup location should house an up-to-date backup copy of the essential data. In the event that the current data center is inaccessible, a backup location should come online and provide the essential services.

- **Current backup copy of the user database and online curriculum**
- **Secondary physical location with a different ISP**
- **Backup location should be available in a short period of time during recovery**
- **Internal server access for employees for updated information during recovery**
- **Each employee should have a local copy of disaster recovery plan**

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.

Answer the following questions:

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

No, the business cannot fully operate without access to the data center. Remote access to the servers within the data center is essential for core business functions, as:

- Customer Access: Customers rely on the data center for logging into accounts and accessing tutoring services and online content. Without this access, they cannot utilize the services, leading to potential dissatisfaction and lost revenue.

- Instructor Access: Instructors also need access to the data center for student records and course materials necessary to conduct tutoring sessions. Without these resources, they cannot provide effective instruction or maintain continuity for students.

Answers will vary. The business requires access to the servers within the data center remotely. Without access, the business cannot function because customers cannot access the tutoring services and the online content. In addition, instructors cannot provide tutoring or access student information.

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

The business can only function in a limited capacity without access to the data center. While in-person tutoring services at staffed physical locations may continue, core online functionalities would be unavailable. This limitation means:

- Restricted Service Availability: Only students who can visit physical locations could receive tutoring, limiting access for remote students and those reliant on online materials.
- Loss of Remote Accessibility: Online tutoring sessions, student records, and digital resources housed in the data center would be inaccessible, severely impacting service delivery for most users.

Answers will vary. The business has limited function if only the staffed physical locations can provide the tutoring services.

Can the students access their online materials? Explain.

No, students cannot access their online materials because the servers hosting these resources are located in the data center, which is currently inaccessible. Without server access, students are unable to retrieve or view the curriculum and learning materials they rely on, disrupting their studies and progress.

Answers will vary. The students cannot access their online materials because access to the servers at the data center is not available.

Can the instructors still provide the tutoring services? Explain.

Yes, instructors can still provide tutoring services if they use alternative meeting applications, such as Zoom, Microsoft Teams, or Google Meet, to connect with students. While they may not have access to student records or specific teaching materials stored in the data center, these platforms allow for basic tutoring sessions to continue. However, the effectiveness of these sessions may be limited without access to the full range of resources typically available through the data center.

Answers will vary. The instructors can still provide services if they can connect with their students via meeting applications that are provided by other online providers.

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

No, new users cannot sign up for the tutoring services if access to the business's online user database or curriculum is required, as these are located in the inaccessible data center. Without access to the database, the system cannot register new users, process their information, or provide access to necessary resources, effectively blocking new client onboarding.

Answers will vary. New users cannot use the service if they cannot access the business's online user database or curriculum.

Can the employees access internal company information during the recovery?

No, employees cannot access internal company information during the recovery if it is stored in the data center. This lack of access restricts their ability to retrieve essential resources, conduct administrative tasks, and communicate internally, which could delay recovery efforts and impact overall operations until full data center functionality is restored.

Answers will vary. The employees have no access to internal information during recovery.

Step 2: Recommend a recovery plan.

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

- Maintain an Offsite Backup: Ensure a current backup copy of the user database and online curriculum is stored at a different physical location or in the cloud. This backup should be regularly updated to allow for immediate deployment if the primary data center is compromised.
- Deployable Server Backups: Keep backup copies of critical servers that can be activated as needed. This approach enables rapid setup of essential services without complete dependence on the affected data center.
- Distribute Local Copies of the Disaster Recovery Plan: Provide each employee with a local copy of the disaster recovery plan, detailing roles, contacts, and response steps, ensuring everyone can operate effectively during a disruption.
- Alternative Communication Channels: Identify and test alternative communication services, separate from those in the data center, to maintain internal and external contact. This includes using cloud-based or third-party communication tools that are independent of the primary infrastructure.

Answers will vary. This business cannot function without access to its user database and online curriculum. In the event of an attack:

- **Current backup copy of the user database, online curriculum at a different physical location**
- **Backup copies of the servers that can be deployed as needed**
- **Each employee should have a local copy of disaster recovery plan**
- **Identification and testing of alternate communicate services to those housed in the data center**

Part 3: Loss of Data

Users have reported that they are unable to login to their accounts, and they were unable to reset their credentials. 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.

Answer the following questions:

Can the business operate with the data loss? Explain.

Yes, the business can continue to operate, but with potential limitations depending on the extent of the data loss.

- Minor Data Loss: If the data loss is limited to recent progress or some user credentials, the business can likely continue operating, though affected users may face inconveniences and temporary disruptions in their learning experience.
- Significant Data Loss: If substantial amounts of user data, class progress, or critical records were lost, the business's functionality would be impaired, potentially impacting user satisfaction, customer support demands, and service quality.

Answers will vary. It depends on the extent of data loss. The business should be able to continue with possible limitations.

Can the students access their online materials? Explain.

Students can access their online materials only if those materials are not part of the lost data and their accounts can be restored.

- Unaffected Data: If the online materials and course content are intact, students with active accounts should have normal access.

- Affected Accounts: For students whose accounts or progress data were lost, access may be restricted until the accounts and data are restored, which could delay or disrupt their learning experience.

Answers will vary. The students can only access their online materials if their online materials are not part of the lost data and their accounts can be restored.

Can the instructors still provide the tutoring services? Explain.

Instructors can provide tutoring services only if their online materials and resources are not part of the lost data.

- Unaffected Resources: If the teaching materials, lesson plans, and student records are still accessible, instructors can continue their sessions with minimal impact.
- Affected Resources: However, if key instructional materials or recent student progress data were lost, instructors may face challenges in delivering effective sessions, as they might lack the necessary context or resources.

Answers will vary. The instructors can only access their online materials if their online materials are not part of the lost data.

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

New users can sign up if the sign-up system, user database, and curriculum data were not impacted by the data loss.

- Unaffected Sign-Up System: If the system for account creation and access to curriculum data is functional, new users should be able to register and begin using the services.
- Impacted User Database: However, if the data loss includes portions of the user database or essential curriculum, the sign-up process might face issues, potentially preventing new user registrations or delaying access to services.

Answers will vary. New users can sign up if they are not accessing the business's online user database or curriculum that is part of data loss.

Can the employees access internal company information during the recovery?

Employees can access internal company information during recovery if this information was not part of the data loss.

- Unaffected Data: If key internal documents, resources, and communication tools are intact, employees should have normal access, allowing them to support recovery and ongoing operations.
- Impacted Data: However, if critical internal information was lost, employees may face challenges in accessing essential data, potentially hindering recovery efforts and regular tasks.

Answers will vary. The employees have access to internal information during recovery if it is not part of the data loss.

Step 2: Recommend a recovery plan.

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

- Implement Multiple Backup Copies at Different Time Intervals: Retain multiple versions of data backups (e.g., daily, weekly) to allow for restoration from the most recent undamaged version. This approach minimizes data loss by providing recovery options based on specific points in time.
- Incremental and Full Backups: Conduct a combination of full and incremental backups to balance storage needs and ensure critical updates are consistently saved. Incremental backups enable quicker restoration of recent data changes, minimizing potential data loss.

- Anti-Malware Software: Deploy robust anti-malware software to protect against malicious code that could corrupt or delete data. Regularly update the software to keep defenses effective against new threats.
- Regular Software Updates and Security Patches: Keep all systems, applications, and databases updated to address vulnerabilities that could be exploited for data corruption or loss.
- Distribute Local Copies of the Disaster Recovery Plan: Ensure each employee has a local copy of the disaster recovery plan, which includes their roles and response steps, ensuring preparedness in the event of a data-related incident.
- Rapid Data Restore Capability on Redundant Equipment: Enable quick restoration by setting up redundant servers or equipment. This setup allows data to be restored and systems to become operational faster, reducing downtime and enhancing overall resilience.

Answers will vary. The business should have daily backups of all the essential data, such as the user database. Multiple backups of the data at different time increments may be necessary because the undamaged data could be in an older backup only.

For example, the data was damaged by the insertion of malicious code by an attacker 2 days ago. The company keeps full daily backups for seven days. The damaged data can be recovered from the backup that this is 3 days old. However, the trade-off for using an older backup is losing the data from the last two days. On the other hand, if the damaged data can be identified and recovered from the backups, the data loss can be minimized if only the damaged data is incrementally replaced from the backups.

Furthermore, software vulnerability and malicious attacks can also cause data loss in addition to human errors and sabotage.

- **Retain multiple copies of the backups taken at different time intervals**
- **Anti-malware software**
- **Keep software up-to-date**
- **Each employee should have a local copy of disaster recovery plan**
- **Rapid data restore capability on redundant equipment**

Reflection

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

   Key Elements for Disaster Recovery Plans in Businesses Using Offsite Data Centers

   - Offsite and Redundant Data Centers: Essential data operations should be housed in offsite data centers, and to safeguard accessibility, data should be mirrored across two or more locations. This

redundancy ensures that if one data center becomes unreachable, business operations can be restored at another location without significant downtime.

- Real-Time Data Mirroring: Implement real-time or near-real-time mirroring of data across these data centers. This approach enables the swift creation of virtual servers at a backup location, facilitating rapid resumption of services.
- Archived Backups for Extended Retention: Retain multiple backups over time, as the most recent backups may include damaged data in certain incidents. Keeping archived backups enables restoration from the last undamaged version, minimizing data loss from corrupted or deleted records.
- Incremental and Full Backup Strategy: To optimize both storage and restoration time, a mix of full and incremental backups should be maintained. Incremental backups allow for recent changes to be restored without recreating full backups.
- Regular Testing of Disaster Recovery Protocols: Regularly test the entire recovery process to ensure that each step works as planned, helping teams refine the procedure and build confidence in a real incident.

One thing that is very important is that essential data operations be housed offsite in a data center. Because that data center could become unreachable, server should mirror data between two or more data centers. In this way, virtual servers can be created at the backup data center so that business operations can be restored as quickly as possible. Of additional importance, because the most current backup may not include damaged or last data that backups be archived for some period of time, so that the last good backup can be restored.

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?

- **Designate Recovery Leads and Responsibilities**: Assign specific individuals to lead the recovery process, with clearly defined roles for each team member. Having accountable leaders ensures that recovery tasks are executed swiftly and efficiently.
- **Regular Testing and Simulation Drills**: Conduct regular testing of the disaster recovery plan to ensure all procedures work as expected. Simulation drills help identify weaknesses, allowing the team to refine steps and build confidence in their ability to respond effectively.
- **Employee Training and Awareness**: Ensure all employees are trained in the disaster recovery process. They should know their roles and responsibilities, as well as the steps to take during different types of incidents, helping them respond calmly and effectively in an actual disaster.
- **Accessible, Up-to-Date Plan**: Keep the recovery plan accessible to all employees, both digitally and in hard copy if necessary. Regularly update the plan to reflect changes in the infrastructure, new threats, and any lessons learned from drills or past incidents.
- **Establish Communication Protocols**: Define clear communication channels and protocols for internal and external communication during a disaster. This includes notifying affected users, stakeholders, and partners, providing timely updates, and ensuring team members remain informed throughout the recovery process.
- **Secure Offsite and Cloud-Based Backups**: Use a combination of secure offsite physical backups and cloud-based solutions to protect data and ensure easy access to backups, even if primary locations are inaccessible.
- **Continuous Improvement**: After every incident or test, review the recovery process to gather insights and update the plan as necessary. Continuous improvement helps adapt the plan to evolving risks and strengthens resilience against future incidents.

Answers will vary. For a recovery plan to be successful, responsible individuals should be assigned to lead the recovery process and perform the recovery measures. The plan should be tested if possible and all the employees should be trained in the recovery process and know what to do in the event of a disaster. The plan should be available for all the employees and be updated as necessary.