

**MASINDE MULIRO UNIVERSITY OF SCINCE AND TECHNOLOGY**

**SCHOOL: COMPUTING AND INFORMATICS**

**DEPARTMENT: COMPUTER SCIENCE**

**MEMBERS**

**OTIENO REAGAN COM/0026/14**

**CONARD MAYAKA COM/0038/14**

**ISAIAH MUTETHIA COM/0032/12**

**OMONDI REAGAN COM/0031/14**

**CHEBURET LIMO COM/0068/13**

**COURSE: DISASTER RECOVERY**

**CODE: CSC 472E**

**TASK: ASSIGNMENT 1**

**SUBMISSION DATE: 31ST JANUARY 2018**

**LECTURER: MS DOROTHY RAMBIM**

**QUESTION 4**

**You have been appointed as a departmental head in-charge of data and information recovery in XYZ organisation. Critically, outline some of the strategic plans you will have for the department.**

Disaster recovery is normally associated with technology only and faces the recovery facility, operating systems, computer hardware, networking, and other infrastructure, application

Software, databases, and records.

To resume back normal business function a firm should have a disaster recovery strategy. This strategy plan should have a disaster detection, notification and coordination processes, communication strategies, alternate computing facilities management as well as disaster recovery plan testing and maintenance methods.

Disaster recovery plan should be practicable dealing with all the processes necessary to resume technology. It should be assigned to a definite individual for continuance. When developing a disaster recovery plan the restoring should be done according to order of priority such that the major systems are recovered first. One should ensure that network resumes first then applications afterwards. This is because applications are dependent of the network. After priority one should consider time required for the systems. The system which requires a 24/7 uptime should be considered first in relation to those that requires less attention

**CHALLENGES TO DISASTER RECOVERY PLANS**

Firms face several challenges from loss of information. Poor planning by the firm by failure to identify systems that anchor the activities of organizations consisting of detailed plans of recovery to the initial position in cases of emergencies impacts negatively on the process of recovery. In most cases, people opt tend to assume that they understand their networks better while they know little about how they are configured and how these networks operate and more specifically how to effectively manage these systems to ensure that they perform optimally. In cases where IT departments separates other departments making difficult to monitor the systems of other departments such that whenever a disaster struck it becomes a problem to detect and identify the cases of the problem. This causes delays and inefficiencies as the firm try to solve this problem leading to loss of important data and poor performance. The firm should design a strategy that allows the management team to have a disaster recovery plan before and after the occurrence of a disaster thus assisting the firm to handle disaster cases.

The following are the strategic plans for the department.

1. **Prepare Your Members for Data Backup:**

You'll need to educate members of the department about where to store their files (in a specific directory on their PC that is backed up or on the central server) so that all files are included in the backup. This will help avoid data loss in case of a disaster.

1. **Prepare your Members for Disaster Recovery:**

Implement relevant training programs for each team dependent upon task, including crisis communications/ media training as appropriate.

This process is ongoing, as team members change.

1. **Identify the emergency response team:**

Identifying a team will ensure that recovery procedures are executed faster in the case of a disaster. The plan must spell out the titles and functions of each team member involved in the disaster recovery process.

1. Creating a table listing all the critical systems within the department, their Recovery Time Objective (RTO) and Recovery Point Objectives (RPO), and any other relevant information from the initial research. The table should include the following:

* The critical system’s name.
* Its RTO and RPO values.
* The threats that are identified for the critical system.
* Prevention strategies.
* Response strategies and recovery strategies.

1. Schedule the backups to be on daily basis. This is to ensure that operations done the previous day is recovered in case of systems failure.
2. Ensuring that data centres and power supplies are replicated so that when one fails the backup picks up the operations, this ensure reliability.
3. **Identifying the legal requirements:** As a first step in managing IT risks, I should be aware of the legal and legislative requirements for business owners. This makes the first step in any recovery plan of any business.
4. **Ensuring there exist business insurance:** this at some point ensures that in case of human risks or natural risks that would cause damage to the hardware that holds data, e.g. the data centre-servers are to be compensated when crisis occur.
5. **Perform recovery tests on the systems**

Perform functional disaster recovery tests on its critical systems in order to determine the weak points and loopholes that may be existing

1. **Outsourced disaster recovery arrangement.**

In case of outsourced systems, the disaster recovery services are to be determined by the statement of work documents. This would create awareness of the security status of the systems and possible measures to undertake towards disaster recovery.

1. **Plan for protective data security framework.**

Plans to ensure a protective data security framework would be put in place to ensure that the departmental data is secure through the installation of backup applications and security features which include firewall, spyware protectors and antivirus applications.

1. Conducting a post-test review to evaluate the disaster recovery response process, to identify and correct any weaknesses, to determine strengths and promote continuous improvements in the disaster recovery process.