|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: LAURIANO, RYAN | DATE PERFORMED: 11/19/2024 | /40 |
| Section: IDC2 | DATE SUBMITTED: 11/21/2024 |

# SYSADM1 – Data Loss

Instruction/s:

Read and analyze the data loss scenarios provided. Create a data recovery plan by providing impact assessment, recovery plan and preventive measures for each scenario. Lastly, answer the reflection question.

**Evaluation Criteria Guide:**

* 1. Impact Assessment:
* Accurately identifies the potential consequences of the data loss.
* Quantifies the potential financial, operational, and reputational impact.
  1. Recovery Plan:
* Proposes a detailed, feasible, and timely recovery plan.
* Includes steps for data restoration, system recovery, and business continuity.
* Identifies the necessary resources and personnel.
  1. Preventive Measures:
* Recommends specific measures to prevent similar incidents in the future.
* Addresses potential vulnerabilities in security, hardware, and software.
* Proposes regular backups, security audits, and employee training.
* Recommends appropriate RAID levels for data redundancy and performance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Impact Assessment** | **Recovery Plan** | **Preventive Measures** |
| A system administrator accidentally deletes a critical database containing customer information while performing routine maintenance. | If a database with customer information gets accidentally deleted, it could cause big problems. Operations might stop, customers might get mad, and the company could face legal issues. It could also cost a lot of money to fix and hurt the company’s reputation. | First, I would stop everything to avoid making it worse. Then, I would use recovery tools to try to get the data back. If that doesn’t work, I would check if there is a backup then try to restore the database from the latest backup and double-check everything is correct. After that, I would make sure permissions are set properly so it doesn’t happen again. I’d also update the team and customers on what’s going on. | To prevent this, I would set up better permissions, so only certain people can access critical systems. I’d also make sure there are regular backups and train everyone on how to handle data safely. Having a system that keeps versions of the database would also help. |
| A major hard drive failure occurs on a server hosting essential business applications, resulting in data loss. | If the hard drive on a critical server fails, it could cause operations to stop, lead to data loss, and cost a lot to fix. It could also upset customers if services are down for too long. | In this case, I would switch to a backup server or use a disaster recovery site to keep things running. I’d replace the broken hard drive and restore data from backups if there is one. After that, I’d test the system to make sure everything works before going live again. | To avoid this, I’d use RAID for redundancy so we can recover even if a drive fails. I’d also check the hardware regularly, keep backups in safe locations, and consider using SSDs, which are more reliable than regular hard drives. |
| A powerful earthquake strikes a data center, causing significant damage to hardware and power infrastructure. | If an earthquake damages a data center, it could destroy hardware, cause data loss, and shut down operations. Fixing everything could take a lot of time and money, and customers might lose trust in the company. | The first step would be to check what’s still usable. Then, I’d switch operations to a cloud-based system or a backup data center while restoring data from offsite backups. Once things are running again, I’d focus on rebuilding or replacing the damaged systems. | To prepare for disasters like this, I’d make sure we have backups stored in safe locations, like cloud servers or data centers in other regions. I’d also use earthquake-proof equipment for our hardware and run disaster recovery drills to be ready. |
| A ransomware attack encrypts critical data, rendering it inaccessible. | A ransomware attack could lock us out of critical data and stop operations. It could cost money to fix, and if sensitive information is leaked, customers might lose trust in us. | I would first isolate the infected system to stop the ransomware from spreading. Then, I’d report it to the right authorities and remove the malware. After that, I’d restore the data from clean, offline backups and check that the system is secure before bringing it back online. | To prevent ransomware, I’d make sure all software is updated, install antivirus tools, and train everyone to avoid phishing scams. I’d also keep multiple offline backups that can’t be affected by ransomware attacks. |
| A system administrator misconfigures a backup system, leading to data corruption and loss. | If a backup system is misconfigured, it could ruin the backups, making it impossible to restore data when needed. This could cause long downtimes and upset customers while costing money to fix. | I would stop the backup process to avoid more issues and recover the data from other backup copies. Then, I’d fix the backup system and test it to make sure it works properly before using it again. I’d explain to customers and stakeholders what happened and how we’re fixing it. | To prevent this, I’d check the backup system regularly and use tools that monitor for any issues. I’d also keep multiple backup copies in different formats, like on the cloud and external drives, and train people on how to set up backups properly. |
| **Reflection Question**  If some data couldn’t be recovered then I would say to the stakeholders about the data’s that can’t be recovered either due to virus or there is no existing backup for me to recover the lost data. I would explain the steps that were taken to recover the data to make sure that they will not have the wrong impression that we are not trying our best. Then take record of this occurrences to ensure that we can improve our backup and recovery systems so that it can be prevented and would not happen again in the future. In order to mitigate the impact either we can check for the usable data’s and implement some actions before blaming each other as this would lead to panic. | | | |

**Grading Rubric**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criteria** | **Excellent (10 pts)** | **Satisfactory (7 pts)** | **Needs Improvement (4 pts)** | **Score** |
| Impact Assessment | Accurately identifies all significant impacts. | Identifies some key impacts but misses others. | Fails to identify significant impacts. |  |
| Recovery Plan | Proposes a comprehensive, detailed, and feasible plan. | Proposes a basic plan but lacks detail or feasibility. | Fails to propose a viable plan. |  |
| Preventive Measures | Recommends strong, specific preventive measures, including appropriate RAID levels. | Recommends some preventive measures but lacks detail or specificity. | Fails to recommend any preventive measures. |  |
| Reflection Question: | Clearly and concisely explains the situation to stakeholders, acknowledging the limitations of data recovery. | Provides a basic explanation but lacks clarity or empathy. | Fails to provide a satisfactory explanation. |  |
| **Total Score:** | | | | **/40** |