|  |  |  |
| --- | --- | --- |
| SCHOOL OF INFORMATION AND TECHNOLOGY | | |
| NAME: Zhaun Gabrielle F. Pasion | DATE PERFORMED: 11/21/24 | /40 |
| Section: IDC2 | DATE SUBMITTED: 11/21/24 |

# 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. | Losing customer data can hurt the company’s reputation, lead to lost sales, and possibly legal issues. Employees may also struggle to continue their tasks without the data they need. | * Restore the deleted database from the most recent backup. * Use recovery tools to retrieve data if backups are unavailable. * Inform relevant teams and customers about the situation if necessary. | * Train employees to handle databases carefully. * Set up regular and automated backups. * Limit access to critical data to only necessary personnel. * Implement backup servers to use in case the main server is inoperable. |
| A major hard drive failure occurs on a server hosting essential business applications, resulting in data loss. | Users operations might stop and employees may not access tools they need to work. Financial losses could happen if services or products are delayed. This is also a major factor to the provider as this experience might create doubt on the customers if they still want to use the provider’s services. | * Use RAID (if implemented) to recover data. * Replace the failed drive and restore data from backups. * Test restored applications to make sure they work properly. | * Use RAID for storage redundancy. * Perform regular hardware checks. * Invest in reliable, high-quality hardware. |
| A powerful earthquake strikes a data center, causing significant damage to hardware and power infrastructure. | The damage to the data center could result in a complete halt to operations, leading to significant downtime and potential permanent data loss if backups are also affected. This would cause financial losses, added costs for repairs or replacements, and potential customer dissatisfaction, harming the company’s reputation. | * Activate the disaster recovery plan, switching to a secondary data center if available. * Assess hardware damage and repair or replace affected equipment. * Restore critical data and systems from cloud-based backups. * Coordinate with power and infrastructure teams to restore operations. | * Store backups in an off-site location or use cloud storage to ensure data safety. * Design data centers to withstand natural disasters (e.g., earthquake-resistant buildings). * Regularly test disaster recovery plans to ensure smooth execution in emergencies. * Use redundant power systems like generators to minimize disruptions. |
| A ransomware attack encrypts critical data, rendering it inaccessible. | Business operations might stop completely. Paying the ransom could be expensive, and the company’s image might be damaged. | * Isolate the infected systems to prevent spreading. * Restore encrypted data from secure backups and change encryption configurations. * Notify authorities and affected parties. | * Use strong anti-virus and anti-malware tools. * Train employees to spot phishing emails. * Keep software up-to-date with the latest security patches. * Use firewalls or IDP/IPS to prevent unauthorized traffic to enter the network. |
| A system administrator misconfigures a backup system, leading to data corruption and loss. | The misconfigured backup system could lead to corrupted or lost data, disrupting daily operations and delaying important tasks. This could cause financial losses due to downtime and the time needed to fix the issue. | * Identify the root cause of the misconfiguration and correct it. * Restore the lost or corrupted data using older, verified backups. * Verify system integrity and test the restored backups before resuming operations. | * Test backup systems regularly. * Use backup validation tools to check for corruption. * Train administrators to manage backup systems correctly. * Use virtual machines to test configurations before implementing them on real devices to prevent damages in case of misconfigurations |
| **Reflection Question**  *How would you explain to your company's stakeholders if, despite your best efforts, some data was still unrecoverable after implementing data recovery measures? What steps would you take to mitigate the impact of this data loss and prevent future occurrences?*  I can explain the situation to our company’s stakeholders by saying that, despite our best efforts and the implementation of data recovery measures, some data remains unrecoverable due to the extent of the issue. I understand how this affects our operations, and we are actively working to minimize further disruptions by prioritizing restoring critical systems and keeping all affected parties updated. To prevent similar incidents in the future, we will enhance our backup strategies by conducting regular tests, ensuring backups are stored in multiple locations, and providing additional training for our team on proper data management and recovery procedures.  Additionally, I can use the “Virus” scenario, as mentioned by Ma’am Kath in our previous lecture-discussion, in case things get out of hand, but only if necessary. | | | |

**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** |