HECTOR CABRA

18896

Assessment 1

contribute to organizational privacy and contingency plans

Task 1:

What factors would need to be considered in determining whether this new system will be critical to the business and what the impact might be if it fails?

Write at least 4 questions you need to consider.

Good impact:

1. Clear Objectives: Define clear and achievable objectives for the system.
2. Reliability: Ensure the system operates consistently and reliably.
3. Scalability: Design the system to handle growth and increased workload.
4. Security: Implement robust security measures to protect data and resources.
5. Usability: Create an intuitive user interface and experience for ease of use.
6. Flexibility: Allow for customization and adaptation to changing requirements.
7. Performance: Optimize system performance to ensure efficient operation.
8. Maintenance: Develop a plan for regular maintenance and updates.
9. Documentation: Provide comprehensive documentation for users and administrators.
10. Support: Offer ongoing support and assistance to users.

Bad side:

If the systems fail, all the date will be lost.

A skilled engineer is required to ensure that the systems work properly.

It will cause the cloud server to fail and shut down.

If the systems are not monitored it will cost millions to the company.

A screenshot of a computer

Description automatically generated

Task 2 :

**What issues need to be considered for backup and restoration of data?**

Backing up and restoring data is critical for ensuring the continuity and integrity of information within an organization or for personal use. Several key issues need to be considered for effective backup and restoration:

1. Data Loss Prevention: The primary purpose of backups is to prevent data loss. Consideration should be given to the types of data being backed up, the frequency of backups, and the backup storage medium to minimize the risk of losing critical information.

2. Data Integrity: Ensuring that the data backed up is accurate and uncorrupted is essential. Employing checksums or cryptographic hashes can help verify the integrity of backed-up data.

3. Data Security: Backup data often contains sensitive information. Implementing encryption measures both during transit and storage helps safeguard against unauthorized access and data breaches.

4. Backup Storage: Choosing the right storage medium for backups is crucial. Factors such as cost, accessibility, scalability, and durability should be considered. Options include on-premises storage, cloud storage, or a combination of both.

5. Retention Policies: Establishing clear retention policies defines how long backups are retained and when they are eligible for deletion. Compliance requirements, data relevance, and storage constraints influence these policies.

6. Backup Frequency: Determining the frequency of backups depends on factors like the rate of data change, the criticality of the data, and the organization's recovery point objectives (RPOs). Regular backups ensure that recent data is recoverable in the event of a failure.

7. Disaster Recovery Planning: Backup and restoration processes should be part of a broader disaster recovery plan. This plan outlines procedures for responding to various types of disasters, ensuring a swift recovery with minimal disruption.

8. Testing and Validation: Regular testing of backup systems and restoration procedures is essential to verify their effectiveness. Simulated recovery scenarios help identify weaknesses and ensure that backups can be restored successfully when needed.

9. Automated Backup Solutions: Employing automated backup solutions reduces the risk of human error and ensures consistency in backup procedures. Automation also facilitates regular backups and simplifies management tasks.

10. User Training and Awareness: Educating users about the importance of data backup and restoration procedures enhances their understanding of their role in maintaining data integrity and mitigating risks.

By addressing these issues comprehensively, organizations and individuals can establish robust backup and restoration strategies to protect their data against loss, corruption, and unauthorized access.

1. **What problems can occur with backing up online transactions?**

Backing up online transactions presents unique challenges due to the real-time nature of transactional data and the need to ensure data consistency and integrity. Some problems that can occur with backing up online transactions include:

**Data Inconsistency**: Online transactions often involve multiple interconnected databases or systems. Backing up transactional data at different points in time can result in inconsistencies, especially if transactions are occurring concurrently during the backup process.

**Data Volume**: Online transactions generate large volumes of data, which can overwhelm backup systems and lead to performance issues. Managing and storing this data efficiently requires robust infrastructure and storage solutions.

**Transaction Rollback and Recovery**: In the event of a backup failure or corruption, restoring online transactions to a consistent state can be challenging. Transactional databases often rely on complex rollback and recovery mechanisms to ensure data integrity during restoration.

**Data Latency**: Performing backups of online transactions can introduce latency and impact system performance. Balancing the need for real-time transaction processing with backup operations is crucial to minimize disruptions to business operations.

**Data Security and Compliance**: Online transaction data often contains sensitive information, such as financial details or personal identifiers. Ensuring the security and compliance of backup data, including encryption and access controls, is essential to prevent data breaches and comply with regulations.

**Continuous Backup**: Traditional backup methods may not be suitable for backing up online transactions in real-time. Implementing continuous backup solutions that capture changes as they occur ensures minimal data loss and provides more granular recovery options.

**Backup Verification**: Verifying the integrity and consistency of backed-up transactional data is critical. Regular validation and testing of backup systems and procedures help identify any issues or discrepancies early and ensure reliable data recovery.

Task 3:

1. How critical is this system to the organisation? Why?

If any system at any organization is down for a long period of time, it might be devastating for all the security measures, a system shut down is quite vulnerable to any kind of attack. The organization must always have a back-up plan for all their data integrity, any sign of data loss could turn into a huge issue with any customer.

1. The person who completed the form claimed that 30 minutes is the maximum time the system can be down. Does this figure apply to a 24-hour trading period?

No system should be shut down or down more than 10 minutes, beyond that time is quite risky to ensure the integrity of any data related to the company.

Task 4:

A small communications company, 4phones, is about to introduce an e-commerce system. A list of the possible threats to the system has been provided below.

Table: Threats

|  |  |
| --- | --- |
| **Threat** | **Category** |
| Hackers attempting to get to the data stored on the site.   * Change data * Delete data * Add fake or wrong data | Ex\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | in |
| Denial of service attacks to bring the service down.  ... | ex |
| Data destruction by any means such as a user deleting a file.  ... | in |
| Misuse of information by internal staff.  ... | in |
| Power problems so site is down.  ... | ex |
| Overloaded site so response is slow.  ... | ex |
| Customers falsifying information to avoid payment.  ... | ex |
| Incorrect information such as wrong prices so customers pay too little.  ... | in |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.  ... | in |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist * ... | Ex\* |
|  |  |

Identify whether they are internal or external and flag with an \* any threats that are also security threats.

All the internal treats are the ones companies should be most aware of. Every single failure inside the company is just a sign of a poor security practice, if a company is not following the security measures all the external hazards are going to be devastating.

Task 5:

You are working for CIT (City Institute of Technology), an educational organisation that has an annual turnover of $2M. They intend to implement a new system to test students using computerised systems. These tests will include vendor exams such as Microsoft MCSE, Novell CNA, etc.

The following are extracts from the business case and other project documentation that has been developed for this project.

Computerised testing system is a competitive and growing area of business. There are currently five test centres in the city in which CIT is located. Anyone can take these tests: studying with the organisation is not a prerequisite. Students only need to give one day’s notice in order to sit the test.

To gain a marketing edge, CIT proposes that:

* students will only be required to give an hour’s notice prior to being tested. The student will call the test centre to be registered on the new system. They will be given a log-in account and a password and can come to the centre at any time after one hour has elapsed. They will pay by credit card or bring cash to the centre where they log-in and take the test.
* the centre will be open between 5 am and 11 pm, seven days a week.
* the centre expects to be able to process 20 students per hour and will make a profit of $100 per student.
* for security reasons, no tests will be stored at a test centre. Each centre will have an ISDN link with each of the vendors who supply the tests. There will be five such links. When a student registers, an automatic message is sent to the vendor and a test is downloaded to a server at the test centre. The centre must pay $50 for this test even if, for some reason, it does not get used. The test will expire after 12 hours.
* if a student passes the test, they will be presented with a certificate, which is printed at the centre. The centre will keep stocks of these certificates for each vendor.
* student information and test results will be stored on the server and each evening at the close of business this information will be sent to the appropriate vendor. Vendors exercise strict control over test centres and any centre that does not follow the contract obligations may have its test facility refused and suffer financial penalties.

The testing centres are viewed as potential ‘one stop shops’ offering, examination preparation courses as well as tests. Students will study a subject and then take the exam all for an exclusive fee. There is a lot of money to be made as students are willing to pay $5,000 or more to become qualified. The organisation aims to process around 200 students per month.

##### What are the critical data and software areas for this system?

* + Questions random select
  + Students’ answers
  + Test results
  + …

##### What are the potential threats to the system and testing facility?

* + Hack the question
  + Get answer key
  + System is going down
  + …

Critical Data and Software Areas:

Question Random Selection: The system needs to efficiently select questions from a database to create unique test papers for each student.

Students' Answers: The system must accurately record and store the answers provided by students during the tests.

Test Results: It's crucial to store and manage the test results, including pass/fail status and scores, for each student.

User Authentication and Access Control: Ensuring that only authorized individuals can access the system, register for tests, and view test results.

Payment Processing: Secure handling of credit card transactions and cash payments made by students for test registration.

Vendor Communication and Integration: Establishing and maintaining ISDN links with vendors for test delivery and sending student information and test results to vendors.

Certificate Printing: Generating and printing certificates for students who pass the tests.

Backup and Data Storage: Properly backing up student data, test questions, and results to prevent data loss and ensure system reliability.

Potential Threats to the System and Testing Facility:

Unauthorized Access: Hackers or malicious insiders may attempt to gain unauthorized access to the system to steal test questions, answers, or student information.

Data Breach: Theft or exposure of sensitive student information, including personal details and test results, could lead to privacy violations and reputational damage.

Test Tampering: Malicious actors might try to manipulate test questions or answers to gain an unfair advantage or compromise the integrity of the testing process.

System Downtime: Technical failures or cyberattacks could disrupt system availability, preventing students from registering for tests or accessing their results.

Vendor Non-Compliance: Failure to adhere to contract obligations, such as timely submission of student data and test results, may result in penalties or loss of accreditation from vendors.

Payment Fraud: Fraudulent transactions or theft of payment information could lead to financial losses for both students and the testing facility.

Equipment Failure: Malfunction or damage to testing equipment, such as computers or printers, could disrupt test delivery and certificate printing processes.

Regulatory Compliance: Failure to comply with data protection regulations or industry standards may result in legal consequences and financial penalties for the organization.

#### Task 6:

Use the following table to complete your evaluation.

Table: preventive and recovery options

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Options** | **Cost (1-5)** | **Business requirement (1-5)** |
| Disasters that stop the centre operating such as fire, flood, earthquake | Backup System in Different location | 5 | 4 |
| Hardware problems that stop system operating | Best quality hardware | 4 | 5 |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | ... |  |  |
| Student not turning up and exam lapses so $50 is lost. |  |  |  |
| ISDN links broken delaying download of exams |  |  |  |
| Hackers who may try to access test data or student data | Fire wall | 1 | 5 |
| Internal unauthorised access to test data or student data |  |  |  |
| Theft or misappropriation of test certificates | ... |  |  |

**Incomplete Information**: Some threats lack corresponding preventive or recovery options, such as "Credit card fraud" and "Theft or misappropriation of test certificates." It's essential to fill in these gaps to have a comprehensive plan.

**Cost and Business Requirement Ratings**: The provided ratings for cost and business requirement are helpful in evaluating the effectiveness and importance of each option. However, they need to be filled in for all options to provide a clear understanding of their impact.

**Specificity of Options**: The options provided should be specific and actionable. For example, under "Hardware problems that stop system operating," the option "Best quality hardware" is too vague. It would be more useful to specify measures such as redundant hardware configurations or regular maintenance contracts.

**Consideration of Cost vs. Business Requirement**: It's important to strike a balance between the cost of implementing preventive measures and their alignment with business requirements. Some options may have a high cost but are essential for meeting critical business needs, while others may provide lower-cost solutions for less critical threats.

**Addressing All Threats**: Ensure that all potential threats are addressed with appropriate preventive and recovery options. This includes both external threats like hackers and internal risks such as unauthorized access or theft.

**Regular Review and Updates**: The preventive and recovery options should be regularly reviewed and updated to adapt to evolving threats and changes in the business environment. This ensures that the facility remains resilient against emerging risks.

**Training and Awareness**: Consider adding options related to employee training and awareness programs to mitigate internal risks such as unauthorized access or misappropriation of test certificates.

In conclusion, while the table provides a framework for evaluating preventive and recovery options for various threats, it requires additional information and refinement to be fully effective in addressing the security and operational challenges faced by the testing facility. Regular review and updates are essential to ensure the ongoing effectiveness of the risk management strategy.

Task 7:

Write some notes to support your RAID recommendation as a method of preventing hardware failure for the 4phones e-commerce project on the following topics:

1. What RAID may give 4phones

* Fault tolerance as regards disk drives
* Improved performance
* No down time for single disk failure
* Hot swap to replace faulty disk

1. Threats to be safeguarded against

* Disk failure
* Multiple controllers also guard against disk controller failure
* Duplicate power supply guards against power supply failure
* If system unit goes down RAID may be quickly connected to another unit.

1. Cost benefit analysis (Assume 50% would go elsewhere if the system is down)

* Orders placed on the web = $100,000 per day
* Assume 50% would go elsewhere if our system down
* Loss = $50,000
* RAID costs only $12,000

…

1. How RAID supports the business

* 24X7 operation is a business strategy
* 99.9% uptime is an SLA requirement
* RAID provides fault tolerance to meet these requirements

The provided notes offer a comprehensive overview of the benefits of implementing RAID (Redundant Array of Independent Disks) for the 4phones e-commerce project, along with the associated threats to safeguard against, cost-benefit analysis, and how RAID supports the business objectives. Here are some observations and conclusions regarding this information:

**Comprehensive Coverage:** The notes cover various aspects related to RAID implementation, including its benefits such as fault tolerance and improved performance, threats to mitigate, cost considerations, and alignment with business objectives. This holistic approach ensures that all relevant factors are considered in the decision-making process.

**Clear Justification:** The notes provide clear justifications for implementing RAID by highlighting its ability to minimize downtime, mitigate the risk of data loss, and meet the business requirement of 24x7 operation and high uptime. The cost-benefit analysis further reinforces the economic rationale for investing in RAID technology.

**Risk Mitigation:** By identifying potential threats such as disk failures, disk controller failures, and power supply failures, the notes demonstrate a proactive approach to risk management. RAID's redundancy features effectively mitigate these risks, thereby enhancing the reliability and resilience of the e-commerce platform.

**Strategic Alignment:** The discussion on how RAID supports the business objectives underscores its strategic importance. RAID technology not only ensures uninterrupted service delivery but also helps maintain customer satisfaction and uphold service level agreements (SLAs), which are crucial for the success of the e-commerce project.

**Consideration of Cost:** The cost-benefit analysis indicates that the investment in RAID technology is relatively low compared to the potential losses associated with system downtime. This highlights the cost-effectiveness of RAID implementation and makes a compelling case for its adoption.

In conclusion, the provided notes offer a compelling argument for implementing RAID as a method of preventing hardware failure for the 4phones e-commerce project. By addressing potential threats, assessing cost implications, and aligning with business objectives, RAID emerges as a practical and effective solution to ensure the reliability, availability, and continuity of the e-commerce platform's operations.

Task 8 :

Revised Virus Protection Procedures and User Operations:

a. Ensure that all devices connected to the network are equipped with the latest antivirus software and have real-time scanning enabled.

b. Regularly update antivirus definitions and security patches across all devices to defend against emerging threats effectively.

c. Implement automated scans on a scheduled basis to proactively detect and remove any malware or suspicious activity.

d. Educate users on safe browsing habits, emphasizing the importance of avoiding suspicious websites, clicking on unknown links, or downloading files from untrusted sources.

e. Enforce a policy requiring the use of strong passwords and multi-factor authentication to enhance account security and deter unauthorized access.

f. Conduct regular cybersecurity awareness training sessions to educate users about common threats like phishing attacks and social engineering tactics and empower them to recognize and report suspicious activities.

g. Limit user privileges to the minimum required for their job function to reduce the risk of malware spreading and unauthorized system modifications.

h. Employ network segmentation and access controls to isolate sensitive data and critical systems from potential threats and contain the impact of any security breaches.

i. Establish a clear incident response plan outlining the steps to follow in the event of a security incident, including reporting procedures and escalation paths.

j. Conduct regular security audits and assessments to evaluate the effectiveness of virus protection processes and user operations and identify areas for improvement.

**Hardware or Software Recommendations for Backup and Recovery:**

a. Hardware: Invest in a dedicated backup server or network-attached storage (NAS) device with sufficient storage capacity to accommodate regular backups of critical data. Look for features like redundant storage drives and RAID configurations to enhance data reliability and fault tolerance.

b. Software: Consider implementing comprehensive backup and recovery software solutions that offer features such as automated backups, incremental backups, and data encryption. Look for solutions that support multiple backup destinations, including cloud storage, to provide additional redundancy and flexibility in disaster recovery scenarios.

c. Cloud Backup Services: Explore cloud backup services that offer off-site storage for backups, providing an extra layer of protection against on-premises disasters like hardware failures or physical damage to infrastructure. Look for services with robust security measures and compliance certifications to ensure the integrity and confidentiality of backed-up data.

d. Disaster Recovery Planning: Develop and regularly update a comprehensive disaster recovery plan that outlines procedures for restoring data and systems in the event of a disaster. Test the plan regularly to validate its effectiveness and identify any gaps or areas for improvement.

e. Training and Documentation: Provide training to IT staff on the use of backup and recovery hardware and software solutions, including proper configuration, monitoring, and maintenance practices. Document backup and recovery procedures in detail to ensure consistency and facilitate troubleshooting in case of issues.

f. Budget Considerations: Allocate sufficient budget for hardware and software purchases, taking into account factors such as storage capacity requirements, scalability, and ongoing maintenance costs. Consider the potential cost savings and business benefits of investing in robust backup and recovery solutions compared to the potential costs of data loss or downtime in the event of a disaster.