Wells International College

Sang ah park  70309

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Sang ah Park | ID | 70309 |

# Assessment 1- Case Study

Contents

[Assessment 1- Case Study 2](#_Toc65661060)

[Instructions 3](#_Toc65661061)

[Scenario 1: identifying critical systems 4](#_Toc65661062)

[Scenario 2: analysing critical areas 4](#_Toc65661063)

[Scenario 3: determining system criticality 5](#_Toc65661065)

[Scenario 4: identifying possible threats 7](#_Toc65661066)

[Scenario 5: identifying critical systems and threats 7](#_Toc65661067)

[Scenario 6: evaluating preventive and recovery options 10](#_Toc65661068)

[Scenario 7: presenting a strategic recommendation 11](#_Toc65661069)

[Scenario 8: reviewing procedures 13](#_Toc65661070)

[Index 15](#_Toc65661071)

# Instructions

This task is to be completed individually. You need to analyse number of case scenario related to professional conduct, Intellectual property, copyright, privacy and contingencies and complete all the tasks or answer all the questions provided after each scenario.

You need Internet access to analyse and complete some of the tasks.

#### Duration:

Trainer will set the duration of the assessment.

**https://one-rainy-day.github.io/COPCP/**

## Image result for develop a website to manageScenario 1: identifying critical systems

A clothing retail organisation, Urban Wear, intends to develop a website to manage orders and payments for its products. It will display a picture of each product, its price and availability. Customers will be able to order and pay for the goods online. The organisation believes that this will extend its sales to other countries and allow 24-hour selling.

#### Task 1:

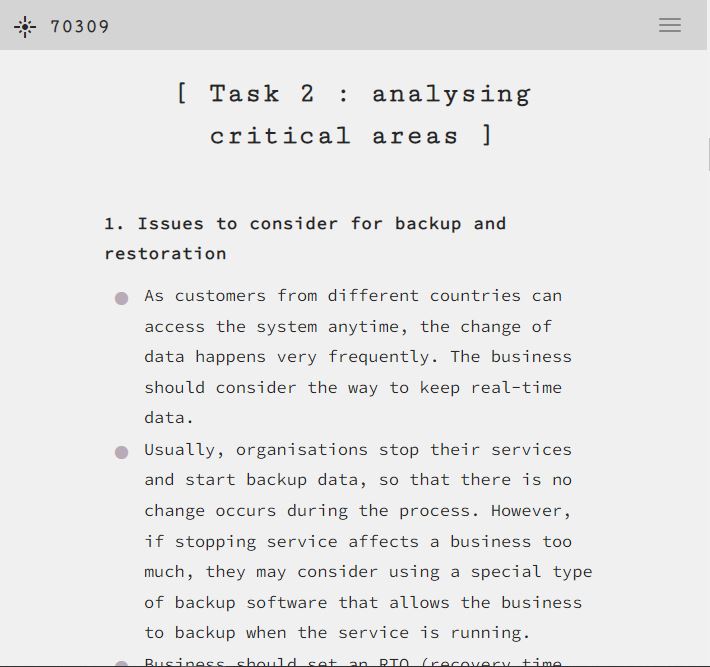
What factors would need to be considered in determining whether this new system will be critical to the business and what the impact might be if it fails?

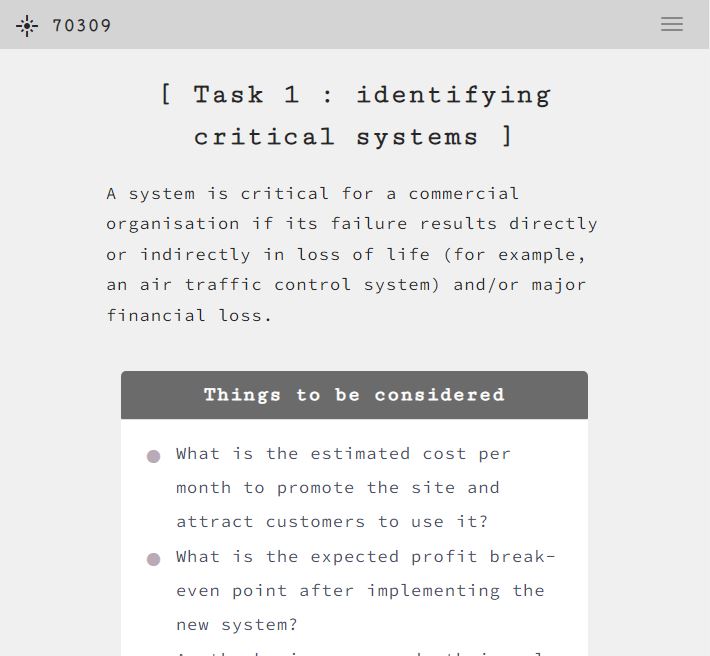
Write at least 4 questions you need to consider.

**Things needed to be considered to determine criticality of the new system:**

1. What is the estimated cost per month to promote the site and attract customers to use it? And what is the expected profit break-even point after implementing the new system?
2. As the business expands their sales routes to other countries, how will they manage inventory, delivery and maintain the quality of customer service?
3. What is the expected quarterly revenue after the introduction of the new system and what percentage of growth is expected to the current system?
4. Will the profits of offline sales be maintained after the introduction of the system? If it is reduced, how big is the threat to the current store? And how will it affect the overall business?

**Expected impacts when it fails:**

1. Decline in sales during periods of system failure
2. Customers lose trust in the brand
3. Legal issues in case of loss of important data



## Scenario 2: analysing critical areas

You have been given the following form for the Urban Wear e-commerce site. Most of the data will be input online via the Internet.

Table 1: critical areas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Update corporate data files** | **Create own data files** | **Create shared documents** | **Create own temporary documents** |
| **From source documents** | 70% | 50% | 20% | 20% |
| **From other data files** | 10% |  |  |  |
| **From irrecoverable sources such a telephone calls** |  |  |  |  |
| **Developed at the workstation such as report writing** | 0 |  |  |  |
| **Other—specify** | 0 | 50% | 50% | 0 |

#### Task 2:

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

* + As customers from different countries can access the system anytime, the change of data happens very frequently. The business should consider the way to keep real-time data.
  + Usually, organisations stop their services and start backup data, so that there is no change occurs during the process. However, if stopping service affects a business too much, they may consider using a special type of backup software that allows the business to backup when the service is running.
  + Business should set an RTO (recovery time objective) and an RPO (recovery point objective) to restore data.

2. What problems can occur with backing up online transactions?

* + Transaction data can be lost between each backup. Consistency of data must be ensured by acquiring all journals in which data update details are recorded. Also, redundancy of storage can be helpful in case of a crash.

## Scenario 3: determining system criticality

Consider the case study of Urban Wear again. You have the following information about its e-commerce system.

Table: Analysing critical areas: impact of system down for less than 1 hour.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Very costly** | **Serious** | **Little or no effect** |
| **Impact on cash flow** | X | X |  |
| **Impact on profitability** | X | X |  |
| **Impact on customer or supplier relations** | X | X |  |
| **Impact on legal requirements** |  |  | X |
| **Impact on staff or morale** |  |  | X |

Some questions and answers related to the impact of critical areas:

* Are there any other implications? Please specify.
  + We expect to do 50% of our business online within one year. As the products we sell are readily available from our competitors, it is likely that customers would purchase elsewhere.
* Estimate the maximum amount of time you could operate without access to the system?
  + 30 minutes
* Are there any peak periods when the impact of a disruption would be more serious?
  + Christmas sales time from mid-November until Christmas Eve.
  + Public holidays
  + School holidays
* Are there any applications or data that you believe must be continuously available?
  + No—subject to no more than 10 minutes downtime

#### Task 3:

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

The information above indicates that the system is highly critical to the business. Because:

* A large proportion of the business depends on their online sales, which is expected to be 50%
* The shorter the period of time before losses start to occur, the more critical the system is. The maximum allowable downtime of the business is only for 30mins and beyond this will severely affect the business.
* As there are other sites that sell the same products, the business should expect a quite big amount of loss of sales and customers (periodically or permanently)
* This may impact their suppliers too.

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?

* It appears to be calculated by average traffic in the country in which the business is based. The volume of traffic must vary largely depending on countries and time zone. To confirm, more data is required.

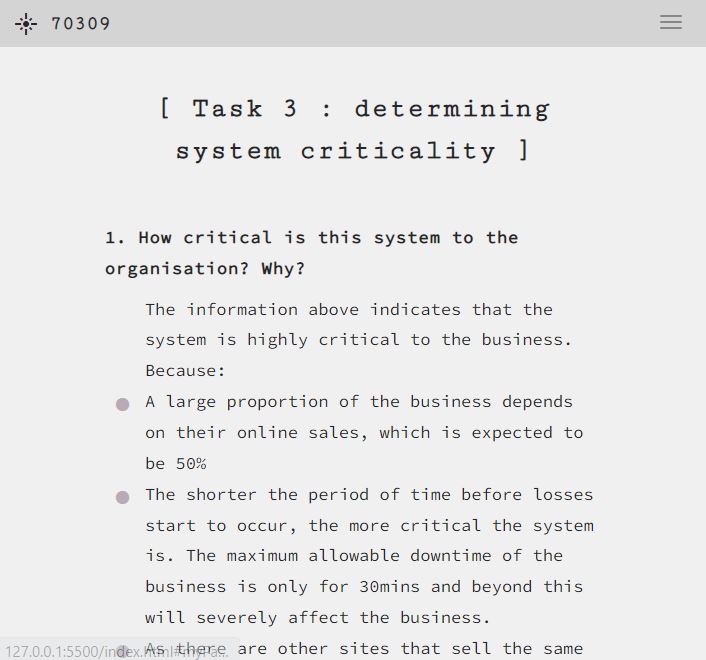
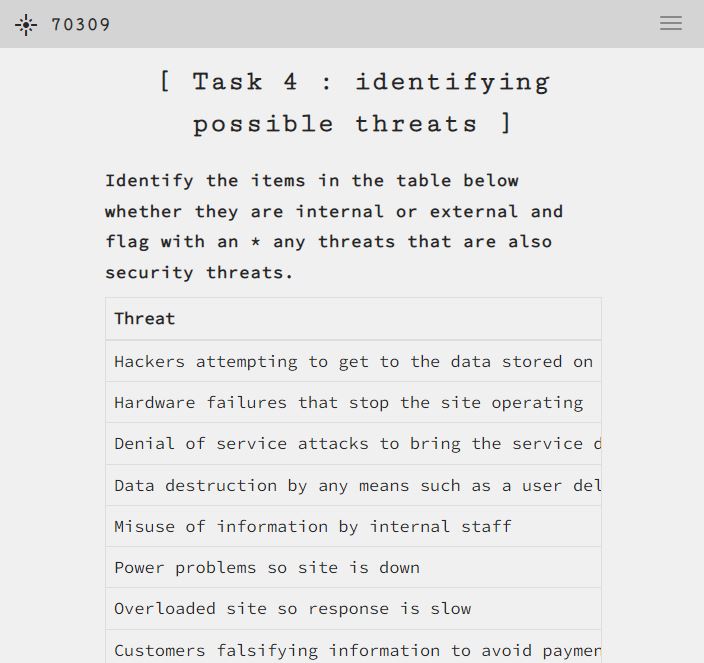
## Scenario 4: identifying possible threats

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.

#### Task 4:

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

|  |  |
| --- | --- |
| **Threat** | **Category** |
| Hackers attempting to get to the data stored on the site.   * Change data * Delete data * Add fake or wrong data | External\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | Internal |
| Denial of service attacks to bring the service down. | External\* |
| Data destruction by any means such as a user deleting a file.   * Accidentally delete file * Intentionally alter data to harm the business * Hardware failure | Internal\* |
| Misuse of information by internal staff.   * Sell customer data to other company * Accidentally expose confidential data to unauthorised people | Internal\* |
| Power problems so site is down. | External |
| Overloaded site so response is slow.   * Low capacity of network * Attackers may intentionally cause overload | External\* |
| Customers falsifying information to avoid payment. | External |
| Incorrect information such as wrong prices so customers pay too little. | Internal |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery. | Internal |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist | External\* |

Comment: Depending on whether the actor was intentional or not, it can be classified as a cyber-attack or accident.

## Scenario 5: identifying critical systems and threats

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.

#### Task 5:

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

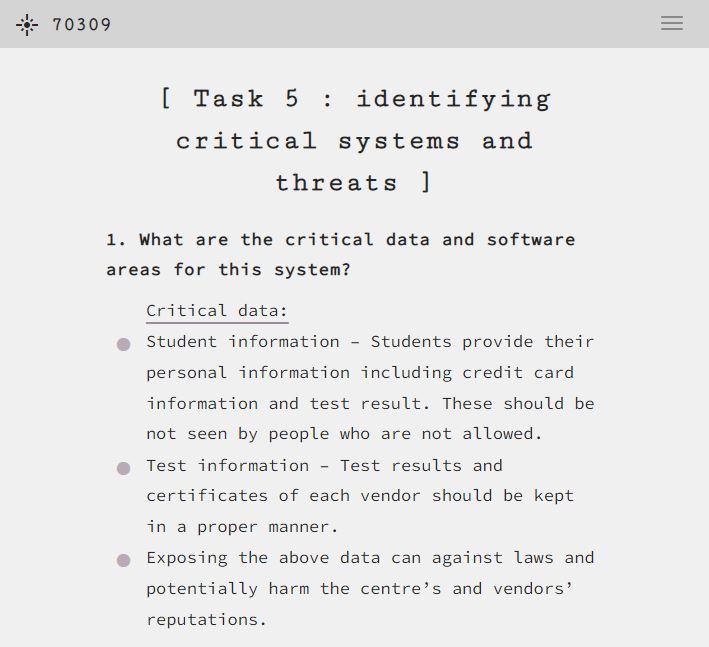
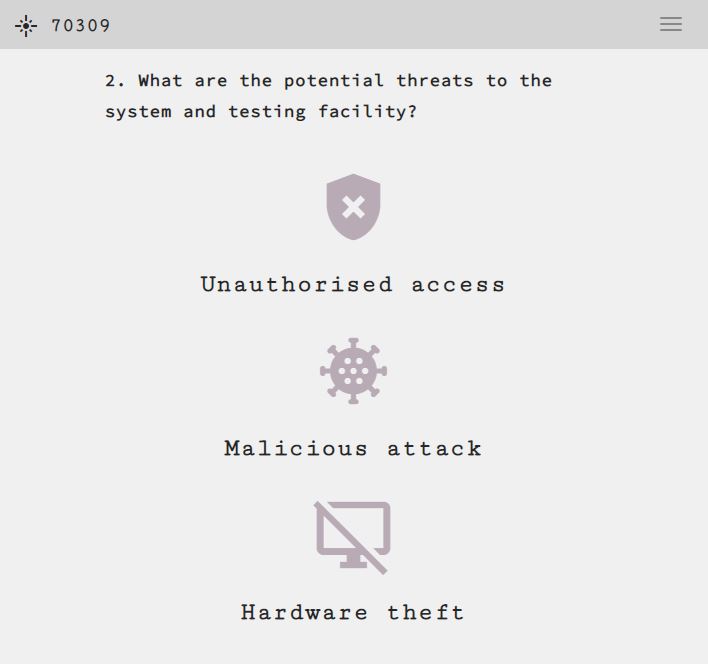
**Critical data:**

* Student information – Students provide their personal information including credit card information and test result. These should be not seen by people who are not allowed.
* Test information – Test results and certificates of each vendor should be kept in a proper manner.
* Exposing the above data can against laws and potentially harm the centre’s and vendors’ reputations.

**Critical software:**

* Booking system –The centre registers students to the system for tests and lets them know their log in ID and password. Having trouble with this, both the centre and students can waste their time and money.
* Test program – As a student login to the test system, the test should be downloaded automatically and starts. If this system doesn’t work or goes down in the middle of the test, it will be crucial.

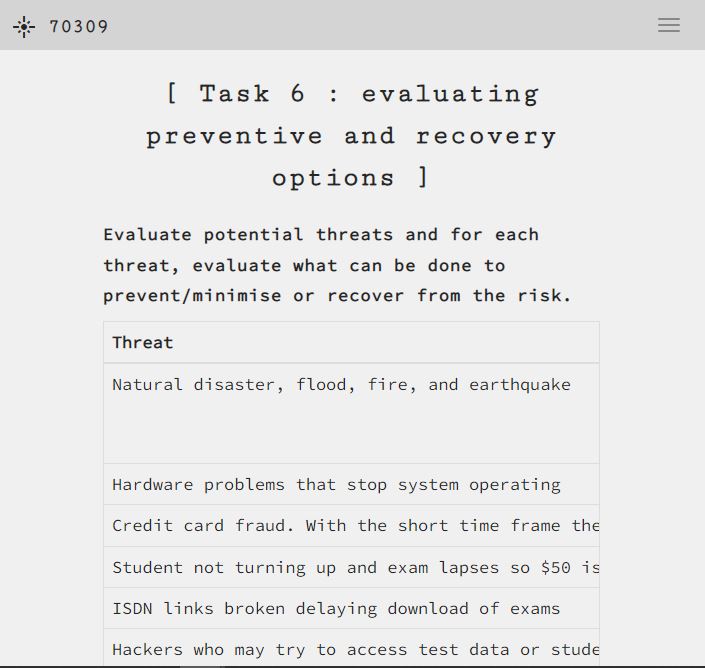
4. What are the potential threats to the system and testing facility?

* Unauthorised access and alteration to critical data
* Malicious software attack on the system
* Theft of hardware
* Damages of facilities caused by various reasons

## Scenario 6: evaluating preventive and recovery options

The Windsor Institute of Commerce (WIC) will implement a new system to test students using computerised testing systems. These tests will include vendor exams such as Microsoft MCSE, Novell CNA, etc.

Before implementing the system, you need to evaluate potential threats and for each threat:

* evaluate what can be done to prevent/minimise or recover from the risk
* consider whether the option would be costly to implement on a scale of 1 to 5 (highest)
* Indicate whether the option should be considered an important or essential business requirement on a scale of 1 to 5 (highest).

#### 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 | System backup indifferent location  Cloud backup | 5  3 | 5  3 |
| Hardware problems that stop system operating | Redundancy of main hardware components | 4 | 5 |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | Use multiple ID to verify the identity | 1 | 3 |
| Student not turning up and exam lapses so $50 is lost. | Charge $50 on booking | 2 | 3 |
| ISDN links broken delaying download of exams | Replace links | 4 | 5 |
| Hackers who may try to access test data or student data | Encryption  Firewalls  Monitoring network | 2  2  2 | 5 |
| Internal unauthorised access to test data or student data | Password protection  Physical protection | 2  2 | 5 |
| Theft or misappropriation of test certificates | Control the number of copies of certificates by using file protection software | 3 | 4 |

## Related imageScenario 7: presenting a strategic recommendation

After completing the risk analysis for the 4phones e-commerce project, you believe that RAID (Redundant Array of Inexpensive Disks) should be used in the server to prevent hardware failure. You also wrote a report that justifies your decision.

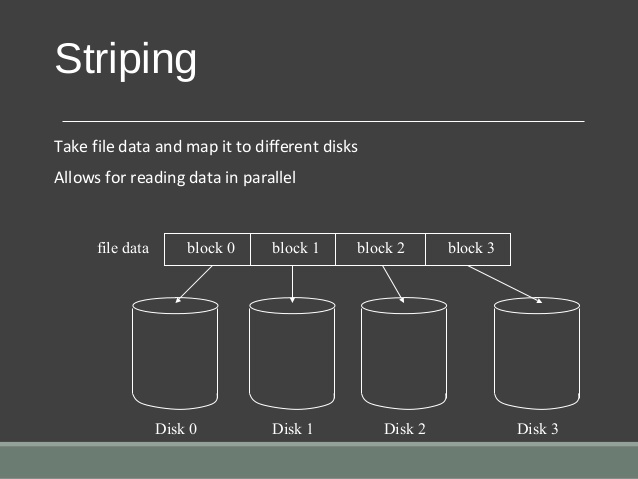
RAID (redundant **array of independent disks**) is a data storage virtualization technology that combines multiple physical **disk** drive components into a single logical unit for the purposes of data **redundancy**, performance improvement, or both.

You covered the following matters in your report:

* The use of RAID will protect against the failure of a single disk in the server. Since disks are electromechanical devices, they are the most susceptible component to wear and tear and subsequent breakdown. They also store the data that may be difficult or impossible to recover depending upon when the breakdown occurs. They will not protect against other hardware failures such as power failures or major disasters such as fire.
* The server has been identified as a critical component in the system and its loss could cause considerable problems and loss of revenue and profit.
* All parts of the system will be impacted by the loss of disks in the server. The cost to the business of losing the server disks for a day could be $100,000. (Orders placed on the web $100,000 per day)
* The only current facility to cope with such an event is to restore from backup. This takes four hours during which time we would not be able to operate the system. In addition, the backup tapes could be on average 12 hours old and so will not have current information.
* While we will eventually have a high-speed link to a backup site, the use of RAID provides a cost-effective solution until this link is established in 10 months’ time.
* The cost of a RAID system would be in the region of $12,000. We will also gain an improvement in the performance of disk access in the region of 10%.
* If this recommendation is approved, we can order the RAID components and have it installed and operating within a week.

#### Task 7:

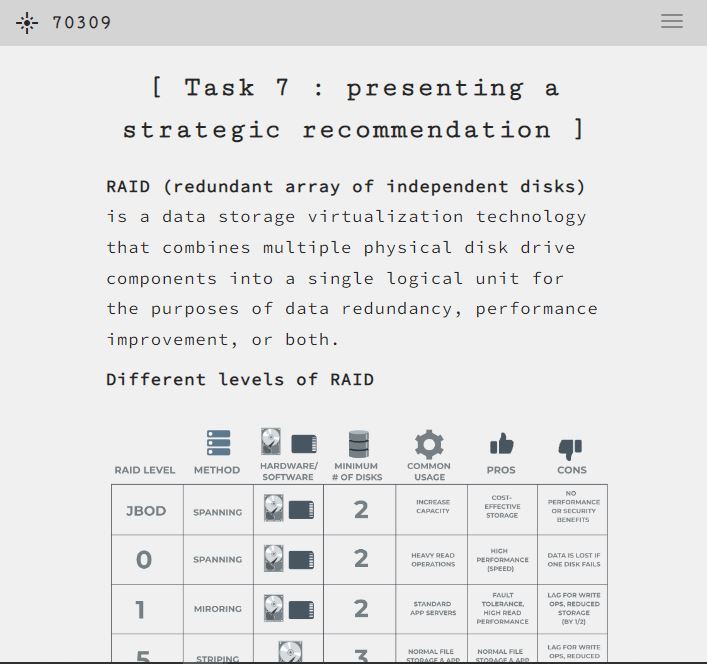
Write some notes to support your RAID recommendation as a method of preventing hardware failure for the 4phones e-commerce project on the following topics:



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

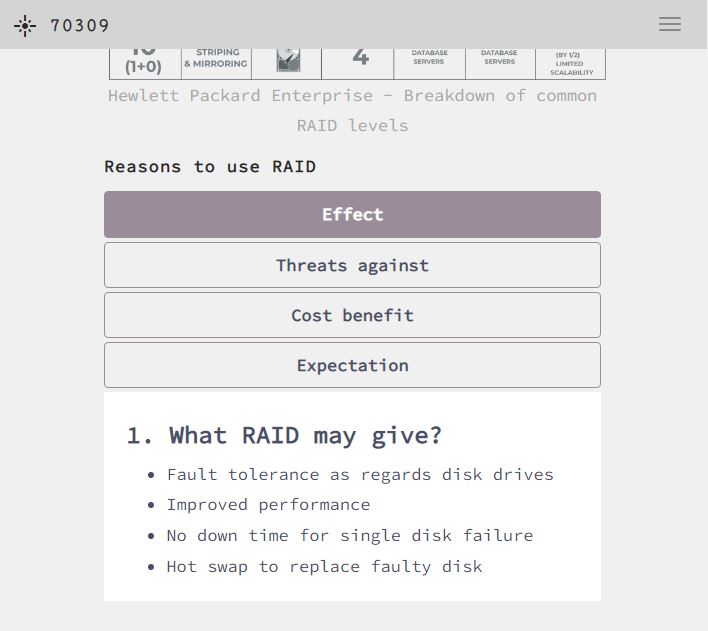
1. Threats to be safeguarded against

* 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

Your comment: There are many types of RAID. Depending on how RAID is configured, it can increase processing speed while giving a single drive with a huge capacity. RAIDs can also increase reliability.

## Scenario 8: reviewing procedures

You have been reviewing the procedures and actual operation of users in relation to virus checking. The current procedures, which were written several years ago, are as follows:

All software loaded on the network should have first been checked for virus contamination. This also applies to shrink-wrapped (brand new) software. The virus checking program selected should be regularly updated to protect against new viruses.

A review of the software and virus files used in checking found the following:

1. The software and files are two years old.
2. No new virus files have ever been obtained.
3. Users only run virus scanning software when they insert a floppy disk.
4. users will often download software from the Internet
5. E-mail is used extensively.
6. Documents are regularly exchanged.

The risk analysis and DRP process recognised viruses as a serious risk that could have a major impact on the organisation.

Viruses can be accidentally or deliberately introduced through infected files or software. Originally only found only in executable programs, viruses can now be carried by other documents, especially Word documents transmitted by e-mail.

New viruses are regularly created and with the increased use of e-mail and the Internet, the risk of a virus attack has also increased. This means that users have to be particularly vigilant and that virus checking of files has to be the norm, not the exception.

#### Task 8:

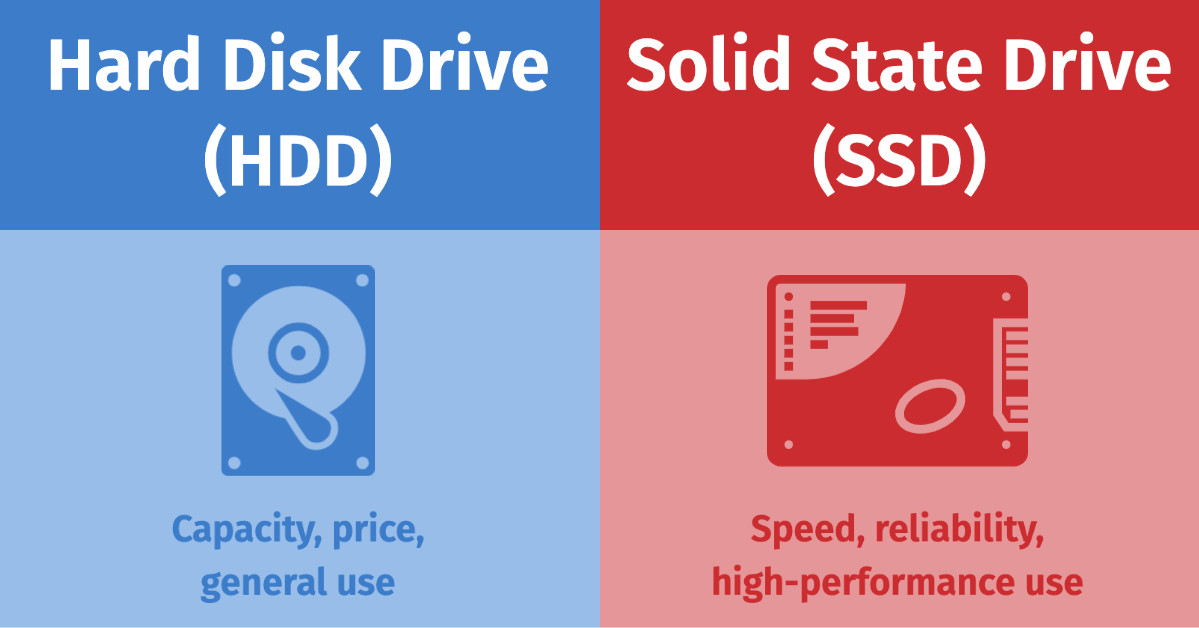
1. Rewrite the procedures to reflect the current virus protection processes and to improve the way users operate.

Computer virus protection procedures

In order to safeguard against viruses, the following procedures must be adhered to by all staff:

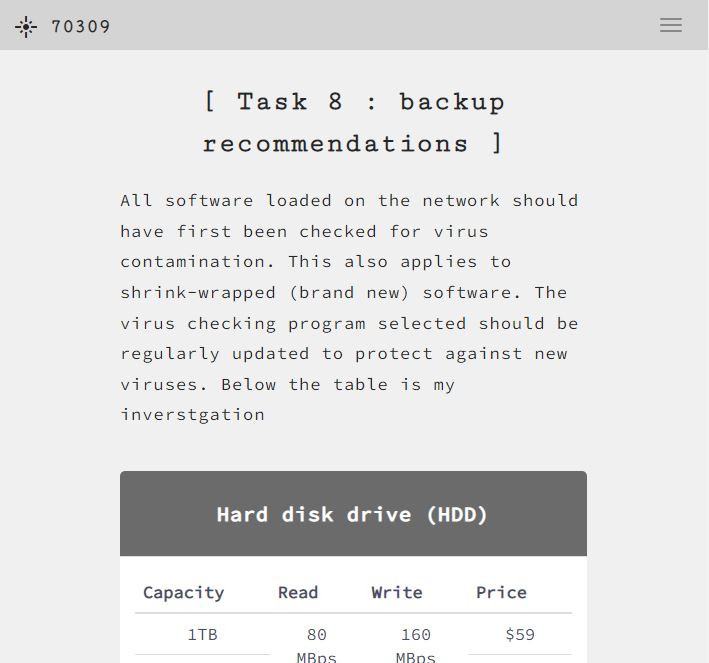
* Standard virus protection software must be installed on all PCs with updates organised automatically through the network.
* Virus protection software must not be stopped or circumvented in any way
* The virus software will be configured to run permanently so that files are always checked prior to opening.
* Any software which recommends that the virus checker be disabled must not be installed without consulting the IT department. Users must never disable the virus checker without authority from IT.
* Applications will be configured to warn of the use of macros, which could be viruses. Macros should only be enabled if the document source can be verified and trusted.
* If any emails or email attachments are received from an unknown e-mail address or if any attachment has macros this should not be opened or macros enabled until the file has been checked by IT.
* The IT department will obtain regular updates (daily) to virus files, which will be installed on the network in order to automatically update workstations.
* All software, whether loaded from a CD-ROM or downloaded from the Intranet, must be scanned before opening.
* If any virus activity is suspected the user must shut down their workstation and inform the IT department.
* All computers will be regularly scanned for viruses on a daily basis as part of the start-up activity.

1. You will need to recommend hardware or software purchases to improve backup and recovery in the event of a disaster.

* Hardware recommendations
*  The current tape unit is too slow and does not have the capacity to store a full back up on a single tape. Typical hardware specifications and costs are:

|  |  |  |
| --- | --- | --- |
| Capacity | Speed(read/write) | Price |
| 1TB | 80~120MBps/  120~160MBps | $59 |
| 2TB | $68 |
| 4TB | $125 |
|  |  |  |
| SSD 1TB | 200~500MBps/  500~1000MBps | $259 |
| SSD 2TB | $459 |
| SSD 4TB | $995 |





## Index

C

configured 11

critical 3, 4, 5, 7, 10

D

duration 2

I

increased 11

N

New viruses 11

O

organisation 3, 4, 5, 6, 7, 10

P

privacy 2

R

recovery 11

S

software purchases 11

U

update workstations 11

V

virus 10, 11

virus protection 11