Wells International College

18268  Daniel Pratama

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Daniel Pratama | ID | 18268 |

# 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.

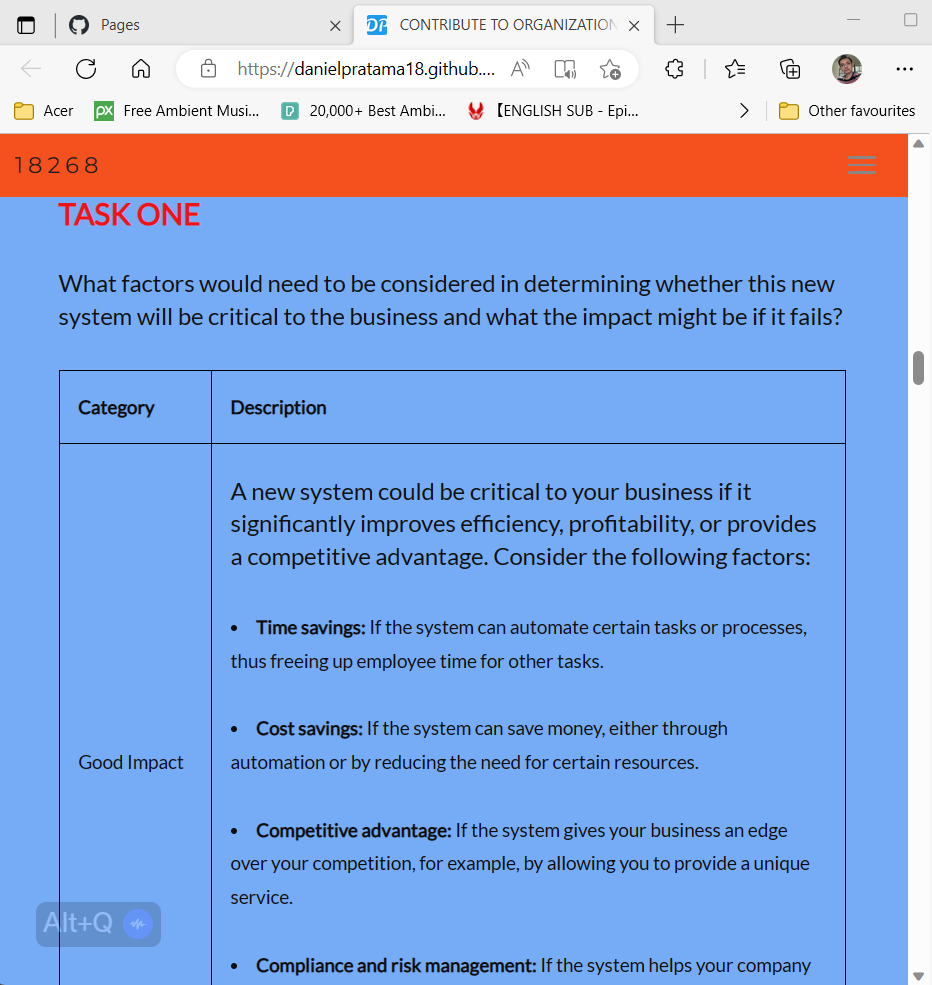
## Scenario 1: identifying critical systems

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.

Good impact:

* **Time savings:**If the system can automate certain tasks or processes, thus freeing up employee time for other tasks.
* **Cost savings:**If the system can save money, either through automation or by reducing the need for certain resources.
* **Competitive advantage:**If the system gives your business an edge over your competition, for example, by allowing you to provide a unique service.
* **Compliance and risk management:** If the system helps your company to comply with regulations and manage risk, particularly in privacy and contingency planning.

Bad side:

* **Downtime:**If the system fails, how long would it take to get it back up and running? What would the impact be on your business during this time?
* **Data loss:**If the system is responsible for storing or managing data, what would the impact of a data loss be? Could it lead to regulatory fines, or damage your company's reputation?
* **Resource drain:**If the system is complex and requires a lot of maintenance, it could consume resources that could be better used elsewhere.
* **Security:**If the system has vulnerabilities, it could expose your business to cyber threats.

Bad side prevented:

* It is reliable and doesn't fail often.
* It is secure and has strong measures in place to protect data.
* It is user-friendly and doesn't require extensive training to use.
* It is flexible and can adapt as your business grows or changes.
* It offers good value for money in terms of its cost versus the benefits it provides.

URL:

<https://danielpratama18.github.io/CopcpBy18268T12023/>

## 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 call** |  |  |  |  |
| **Developed at the workstation such as report writing** | 0 |  |  |  |
| **Other—specify** | 0 | 50% | 50% | 0 |

A screenshot of a computer

Description automatically generated with medium confidence

#### Task 2:

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

* Important data is backup daily base
* At least need three different version stored different locations
* Fast and reliable hardware to support backup
* Backups contain sensitive information and should be encrypted and secured. This includes both physical security for on-site backups and cybersecurity for cloud-based backups.

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

* Did not shut down or close link
* Data has been written during backing up
* Software did not do good validation when transaction occur
* Ensuring that backups are successful and usable can be more difficult with transactional data due to its dynamic nature. Regular tests and verifications are required.

## Credit Card Transaction Processing Online Payment System Ppt PowerPoint Presentation Show - PowerPoint Templates

You comment: ???

## 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



#### Your comment:

Implement system monitoring and alerts to identify and address potential issues before they result in significant downtime. This should provide you with a real-time view of system performance and potential bottlenecks or failures.

#### Task 3:

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

???

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?

I think during

* Weekend or public holiday, max is 10 minutes
* Normal working days, max is 30 minutes
* At night or mid night or before 6 am, max is 60 minutes.
* In order to make your custom happy, you need minimize your server down times.
* Implement continuous monitoring of system performance and set up alerts for potential issues to catch and resolve them before they lead to significant downtime.

## 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.

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.   * Use services like Cloudflare or AWS Shield that can detect and mitigate these attacks. * Implement rate limiting for your server or APIs. | ex |
| Data destruction by any means such as a user deleting a file.   * Regular backups and implementing a robust disaster recovery plan can help recover lost data. * User access controls and tracking can prevent unauthorized data deletion. | in |
| Misuse of information by internal staff.   * Implement strict access controls and user roles. * Regularly audit data access and usage. | in |
| Power problems so site is down.   * Use of uninterruptible power supply (UPS) systems and generators. * Consider hosting your site on cloud services that have measures in place to deal with power outages. | ex |
| Overloaded site so response is slow.   * Use load balancers and auto-scaling to distribute and handle heavy traffic. * Implement CDN for static resources. | ex |
| Customers falsifying information to avoid payment.   * Implement strong user verification procedures. * Use trusted payment gateways. | ex |
| Incorrect information such as wrong prices so customers pay too little.   * Implement thorough testing procedures for site updates. * Use real-time inventory and pricing management systems. | in |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.   * Just like with pricing, real-time inventory management systems can help. * Regularly reconcile physical and digital inventory. | in |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist * Implement a disaster recovery plan that includes data backups and redundant systems. * Consider using multiple data centres in different geographical locations to protect against regional disasters. | Ex\* |
|  |  |

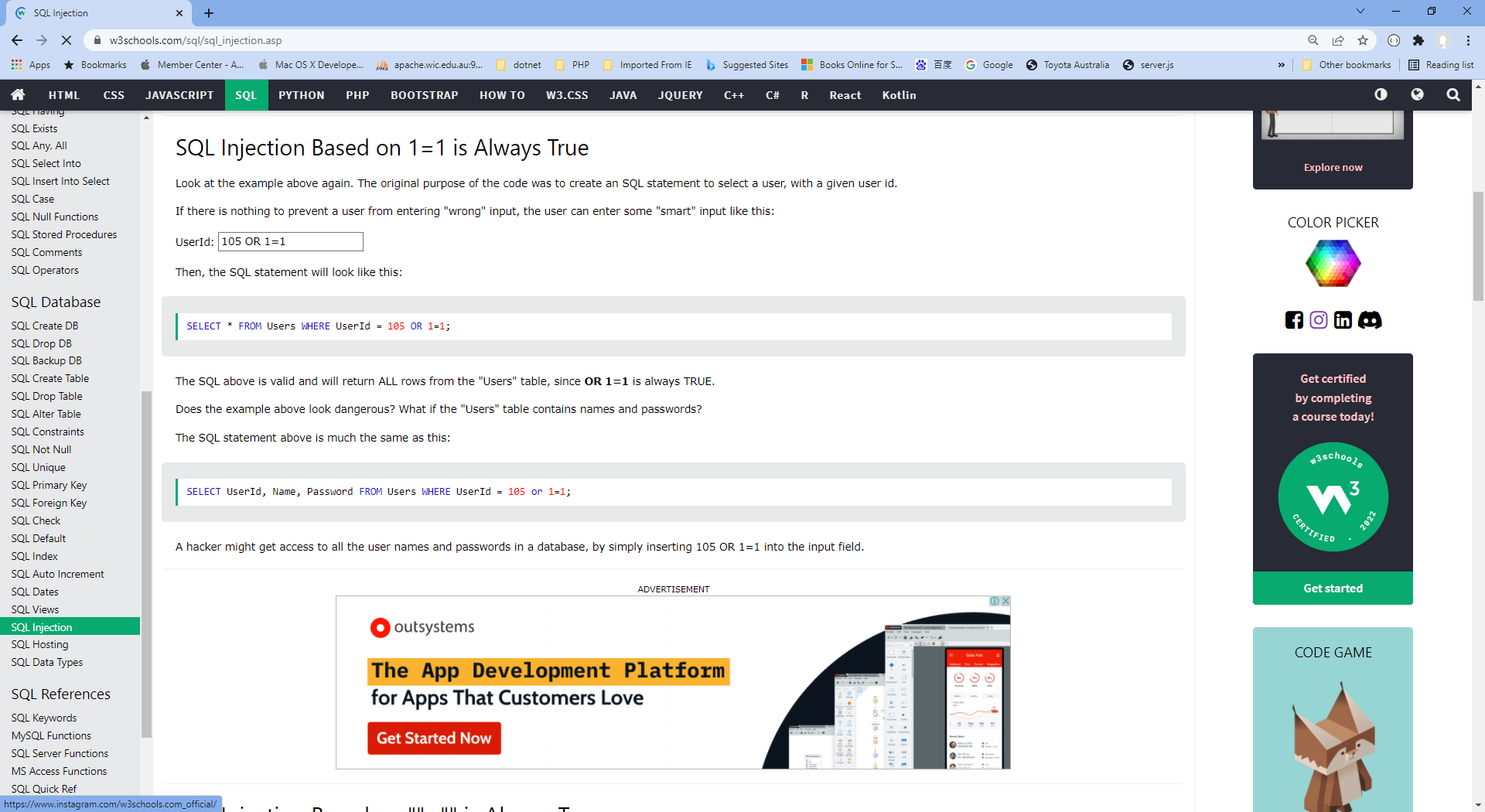
#### Task 4:

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

Example:

SQL injection:

<https://www.w3schools.com/sql/sql_injection.asp>



## Your comment:

SQL injection is a technique where an attacker inserts malicious SQL code into a query. It's a major security vulnerability that can occur in data-driven applications. The attack can lead to unauthorized viewing of data, data manipulation, and data deletion.

* SQL injection usually occurs when you ask a user for input, like their username, and instead of a username, the user gives you an SQL statement that you will unknowingly run on your database.
* SQL injection is a common web application vulnerability because when a developer uses parameters that a user can manipulate without proper safeguards, an attacker can exploit this with malicious intent.
* Attackers can use SQL injection vulnerabilities to bypass an application’s security measures. For example, they could use this technique to bypass login algorithms that are vulnerable, to insert, update, or delete records in a database.
* SQL injection can lead to serious consequences, such as disclosing confidential information, modifying important data, or even issuing commands to the operating system in some cases.
* To protect against SQL injection, developers should use SQL parameters. SQL parameters are values that are added to an SQL query at execution time, in a controlled manner.
* The linked W3Schools page provides sample code for using SQL parameters in PHP and .NET, two common server-side scripting languages.

In short, SQL injection is a serious security vulnerability that can be prevented by using proper security practices, such as validating user input and using parameterized queries.

If you do not know about this, please go to: <https://www.w3schools.com/sql/sql_injection.asp>

## 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:

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

* + Questions random select
  + Students’ answers
  + Test results
  + User Profiles
  + Test Generation and Delivery Software

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

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

Your comment:

To mitigate these risks, it's essential to have robust cybersecurity measures, regular system maintenance, and a comprehensive plan for data backup and recovery. For maintaining test integrity, measures such as remote proctoring, randomizing question order, and sophisticated plagiarism detection could be employed.

## 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 | 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. | Real-time Fraud Detection System | 3 | 4 |
| Student not turning up and exam lapses so $50 is lost. | Online Scheduling and Cancellation System with Late Cancellation Penalty | 2 | 3 |
| ISDN links broken delaying download of exams | Redundant Communication Links | 4 | 4 |
| Hackers who may try to access test data or student data | Fire wall | 1 | 5 |
| Internal unauthorised access to test data or student data | Access Control Systems and Audit Trails | 2 | 5 |
| Theft or misappropriation of test certificates | Digital Certificates with Blockchain Validation | 4 | 5 |

Comment: …

The evaluation of potential threats and their preventive and recovery options displays a comprehensive approach to risk management.

1. For disasters like fires, floods, or earthquakes, the strategy of maintaining a backup system in a different location is cost-intensive but crucial for ensuring business continuity.
2. High-quality hardware has been considered to prevent system operation disruption due to hardware issues. This option also requires a substantial investment but ensures seamless business operations.
3. To counter the threat of credit card fraud, real-time fraud detection software could be employed. Though there's a moderate cost involved, it is essential to secure financial transactions and foster customer trust.
4. Implementing an online scheduling and cancellation system with a late cancellation penalty can prevent monetary loss due to students not turning up for exams. This system is a cost-effective solution to manage exam schedules and minimize losses.
5. Redundant communication links are an effective solution to prevent delays in downloading exams due to broken ISDN links. Despite the high cost, maintaining uninterrupted communication is integral to the business operation.
6. Using firewalls to prevent hackers from accessing test or student data is an affordable yet vital aspect of cybersecurity.
7. Access Control Systems and Audit Trails provide a moderate-cost solution to preventing unauthorized internal access to sensitive data, an essential factor to ensure data security and compliance.
8. The strategy of using Digital Certificates with Blockchain Validation to prevent theft or misappropriation of test certificates is cost-intensive but is crucial to maintain the credibility and integrity of the test certificates.

While some of these preventive measures require significant investment, the costs are justified by the criticality of the business requirements they cater to. Moreover, it is important to remember that the costs associated with these preventive measures often pale in comparison to the potential losses that these threats, if realized, could inflict on the business. Therefore, these investments should be seen not as expenses but as essential elements in safeguarding the business's continuity, integrity, and reputation.

## Scenario 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.

#### Image result for Redundant Array of Inexpensive Disks 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: …

## 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.
7. ...

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.

#### Image result for computer virus warningTask 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.

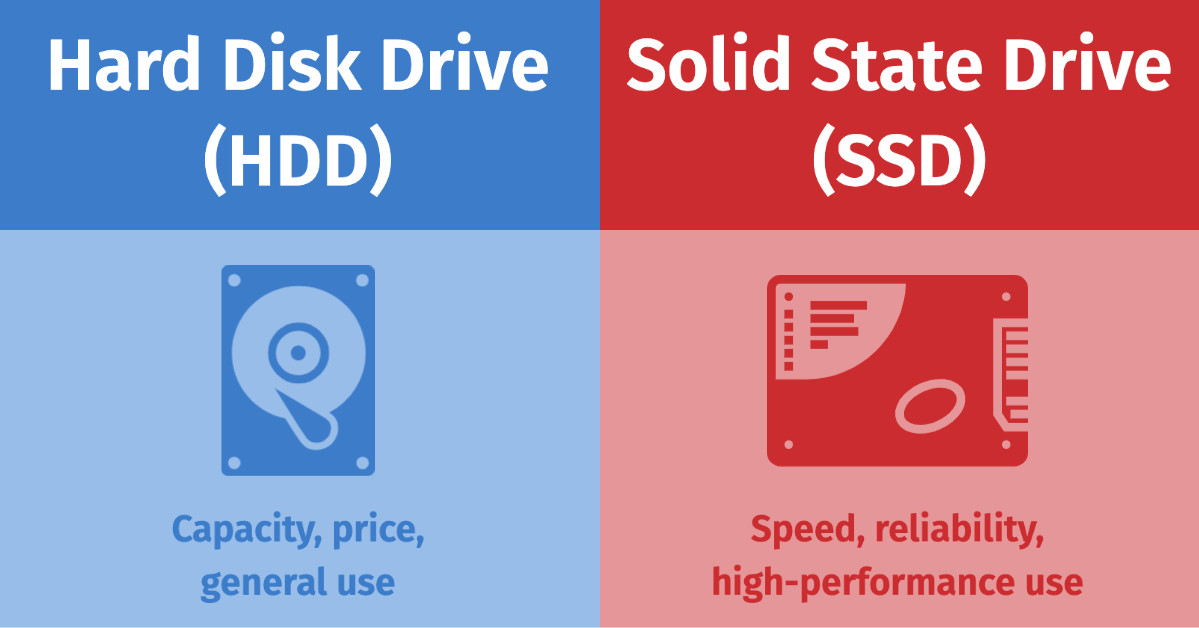
The IT department will obtain regular updates (daily) to virus files, which will be installed on the network in order to automatically update workstations.

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 | ... | $59 |
| 2TB | ... | $79 |
| 4TB | ... | ... |
| 8TB | ... | ... |
| SSD 1TB | Read speed 3,500 MBps max. Write speed 2,500 MBps max. | A$298 |
| SSD 2TB |  |  |
| Cloud Server | Internet upload and download speed | Monthly or Yearly Cost? … |

[https://wellsjohn220.github.io/copcp/#taskeight](https://wellsjohn220.github.io/copcp/%23taskeight)

A screenshot of a computer

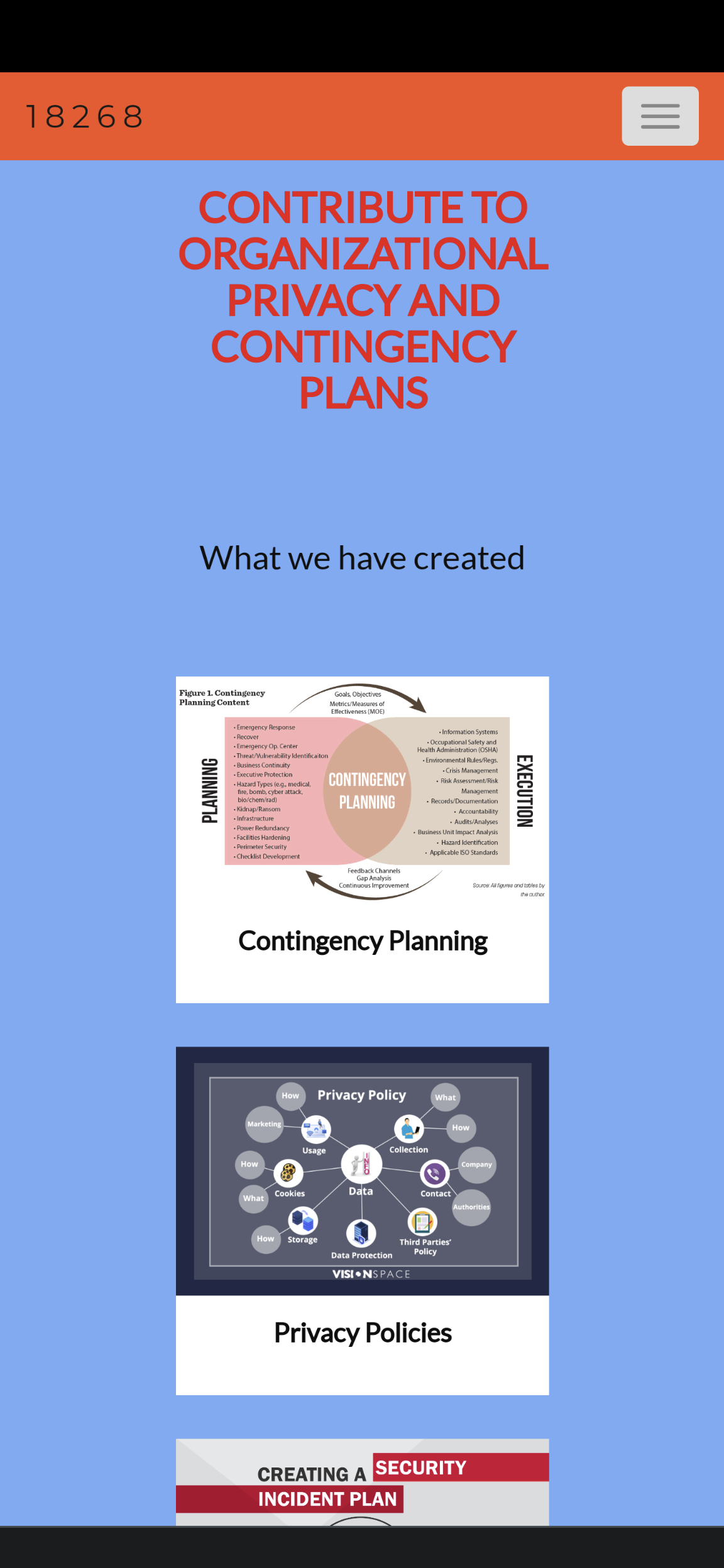
Description automatically generated

Below these is my web contents support.

A picture containing text, screenshot, software, web page

Description automatically generated

A picture containing text, screenshot, font, graphic design

Description automatically generated

<http://supercodepower.host20.uk/Copcpwebsite/>

## 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