31 May 2022

Contribute to Organizational Privacy and Contingency Plans

Assessment One

Full Name: Artur Nagaev Student ID: 70230

WELLS INTERNATIONAL COLLEGE

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Artur Nagaev | ID | 70230 |

**Assessment 1 – Role Play**

Contents

[Scenario 1: Identifying critical systems 3](#_Toc104717944)

[Task 1: 3](#_Toc104717945)

[Scenario 2: Analysing critical areas 4](#_Toc104717946)

[Task 2: 5](#_Toc104717947)

[Scenario 3: Determining system criticality 6](#_Toc104717948)

[Task 3: 6](#_Toc104717949)

[Scenario 4: Identifying possible threats 7](#_Toc104717950)

[Task 4: 8](#_Toc104717951)

[Scenario 5: Identifying critical systems and threats 8](#_Toc104717952)

[Task 5: 9](#_Toc104717953)

[Scenario 6: Evaluating preventive and recovery options 10](#_Toc104717954)

[Task 6: 10](#_Toc104717955)

[Scenario 7: Presenting a strategic recommendation 11](#_Toc104717956)

[Task 7: 11](#_Toc104717957)

[Scenario 8: Reviewing procedures 12](#_Toc104717958)

[Task 8: 13](#_Toc104717959)

[Index 19](#_Toc104717960)

#### 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.

|  |  |  |
| --- | --- | --- |
| ***Considered factors and new system uses*** | | ***Impact*** |
| **Processes** | * customer acquisition * payments, transaction system * customer engagement * delivered services in tangible form | * EFTPOS uses electricity and needs access to a phone network. This payment method will be unavailable if these systems go down. * Depending on where your business is, reliance on electricity or telecommunications can be an important factor to consider. * **Customer preferences** – choosing a payment method that your customers prefer will make them more likely to pay on time. |
| **Infrastructure** | * operating system * telecommunication system (24/7) * technically qualified workforce * internet connection and servers | * Software requires a minimum hardware platform to work properly. * a reliable networking connection to ensure the system shut down. |
| **Operating data** | * optimizing key metrics and business analysis & customer insights * protection customers’ data system * security and safety of business transaction system | * threats involved in transactions by Hacking, impersonation, and viruses, (misuse of encryption or digital signatures |

1. **Is it safe for the information, such as customer credit card details?**

Security problem, such as Credit Card Fraud. It occurs when a hacker gains unauthorized access to customers’ personal and payment information. To access this data, the hacker may penetrate the database of an e-commerce site using malicious software programs. At times, a hacker’s intention when stealing customer’s data is to sell it on black markets.

Is the website have the ability to protect the customer information? For instance, Ticketmaster, one of the biggest online ticket sales and distribution company, admits that their customer details may have been stolen in hacker in last year.

1. **How to define the 24-hour access?**

A website has to be able to respond to the device that it is being viewed on, both in terms of appearance and usage. It is an effective customer experience management platform. A single website should be able to load in different layout formats depending on the device that is loading it, but the content should be taken from a single consolidated source.

* Additionally, the companies also need to consider whether the company is able to respond all their customer for customer service for 24 hour or not?
* Will deliveries be made 24 hours a day?
* Can the organisation’s current distribution resources cope with overseas orders?

1. **How the new system will impact the brand?**

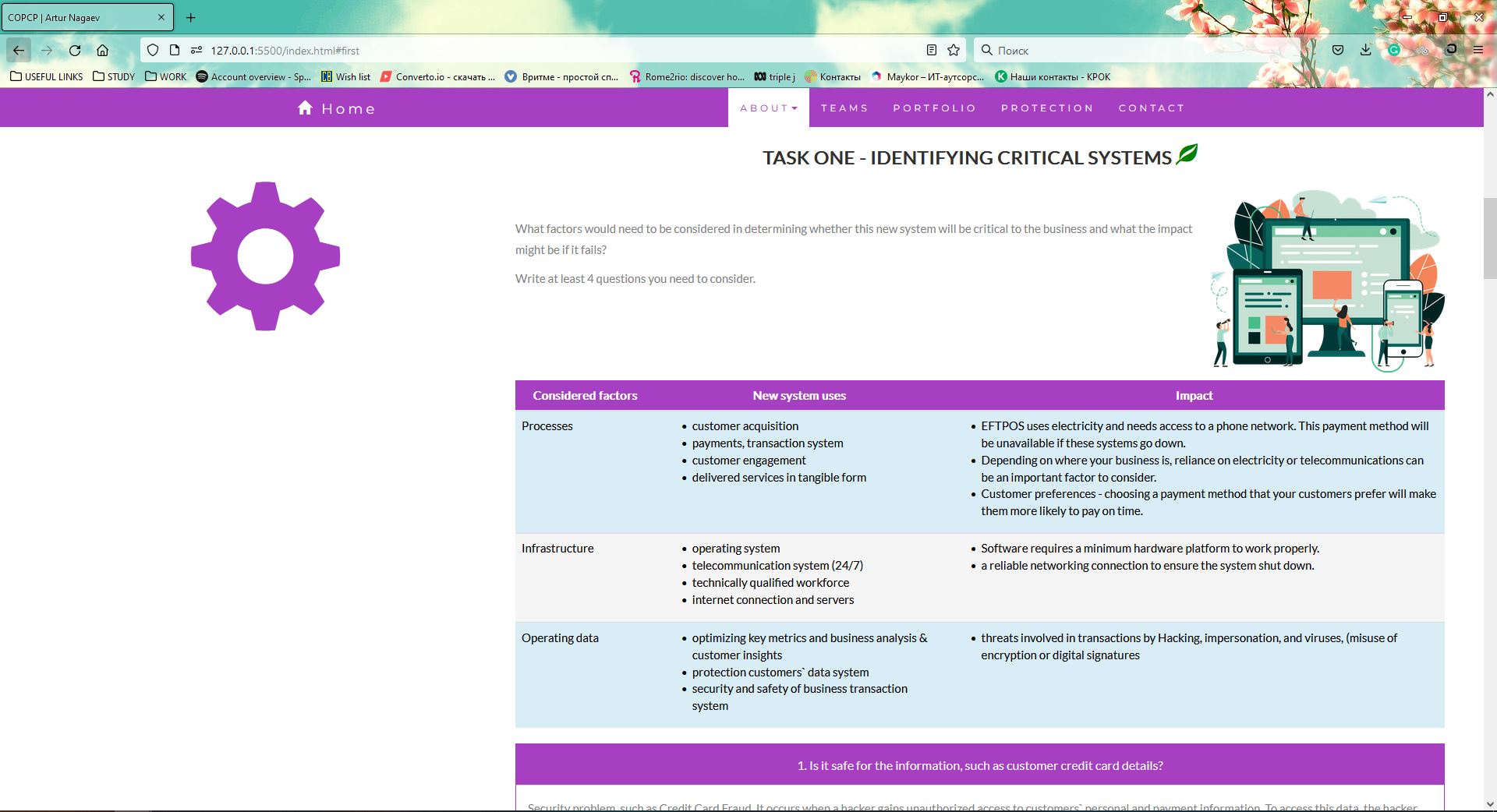
A website should clearly display both the brand and the identity of an organization. The tone of voice and the company branding should be consistent throughout. Further branding can be achieved through social media integration. If the loyalty customer did not like the new system.

Will the customers prefer to visit a store rather than to use the website?

1. **How will the new system impact traditional sales?**

* Will customers prefer to use the website rather than visit a store?
* How will this affect the profitability of the stores?
* If it reduces their profitability, what will happen to the stores?

1. **What volume of sales is the new system expected to generate, especially compared to traditional sales?** (The higher the percentage of overall sales it generals, the more critical the system will be).

****

**Please refer:** <https://artnfur.github.io/copcp>

## 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** | 10% | 50% | 20% | 20% |
| **From other data files** | 10% | 0 |  |  |
| **From irrecoverable sources such a telephone calls** | 80% | 0 |  |  |
| **Developed at the workstation such as report writing** | 0 | 0 |  |  |
| **Other—specify** | 0 | 50% | 50% | 0 |

### Task 2:

1. **What issues need to be considered for backup and restoration of data?**
2. When an organization backs up its data there are three important necessities:

* Confidentiality-the data cannot be accessed by anyone other than authorized personnel;
* Integrity-conservation of the data and protection from unauthorized alterations; and
* Availability-access to the data by authorized personnel.

1. Deal with rapidly increasing amounts of data. Assuming the amount of data being generated continues to increase, it is essential to have backup arrangements that are scalable and that such scalability is cost-effective. This is especially true of infrastructure elements such as virtual environments that are increasingly prevalent in corporate settings.
2. Design and implement a backup infrastructure that maps to business requirements.
3. The system is planned to be available on a continuous basis. This means that special backup arrangements may need to be considered. These may require the system to be down for a brief period during backup or the use of backup software that can backup files in use.
4. **What problems can occur with backing up online transactions?**
5. Using the wrong backup method

The two basic methods for backing up: Exchange data are online and offline. Online backups use a Microsoft interface to copy the selected Exchange data while the Exchange services are running and while the target database is mounted and active. The Exchange-provided APIs backup transaction logs and truncate the logs when necessary.

1. Not verifying Backups

If your backup fails and no one notices, does it make a sound? Maybe not, but your users will surely sound off if you can't recover their mail data.

1. Mismanaging the Transacting Logs

Your ability to restore an Exchange database depends on the state of the transaction logs. If you have the correct set of log files for a database, you have a good chance of restoring the database to the point of failure. Conversely, if the logs are lost or damaged, the odds of a complete recovery drop. When you perform a restore, Exchange attempts to play back the log files, in sequence, from the first log required for the database to the last log. If a log file between the low and high anchor logs is missing, log playback stops. The restore can't continue until you recover the missing log file.

1. Not Allowing Enough Time

Backups take times. Each backup configuration has a throughput number that reflects how much data you can back up and restore in a given time period.

1. Forgetting the small stuff

Exchange backup discussions often focus only on backing up and restoring Exchange data, ignoring the numerous other objects and data items that you must also backup and restore.

1. Not Practicing

The best time to learn how to recover data in your environment is before you have a problem.

## Scenario 3: Determining system criticality

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

Table 2: 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?**

According to the table, this system would be critical to the organization. The revenue and profit is stand for a high proportion, after a year or so of operation. Also it is hard to get loyalty customers through the online store, which easy for online shopper to change to another website to do some shopping, if the system is not available. In the same way, if this system performs better than those of competitors, there is an opportunity to gain some new customers.

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?**

The figure may not apply outside normal trading hours. Even a system that claims to be operating 24 hours, there are a number of uncontrollable factors, still has periods of low activity. According to questions, there are some peak periods when the impact of a disruption would be more serious, which is Christmas sales time from mid-November until Christmas Eve. It may be worth analysing this further. Nevertheless, the system would be considered critical.

## 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.

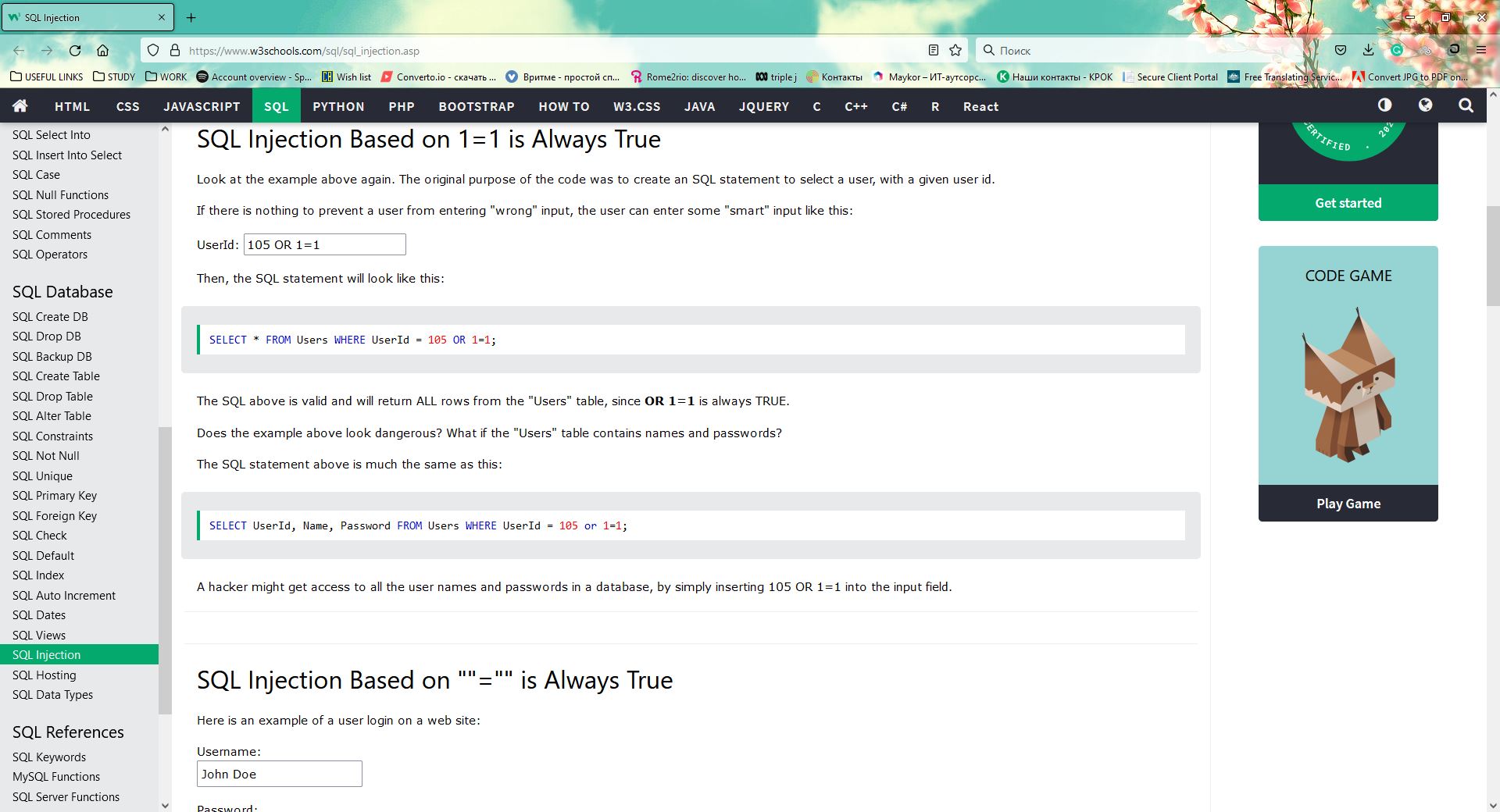
Table 3: Threats

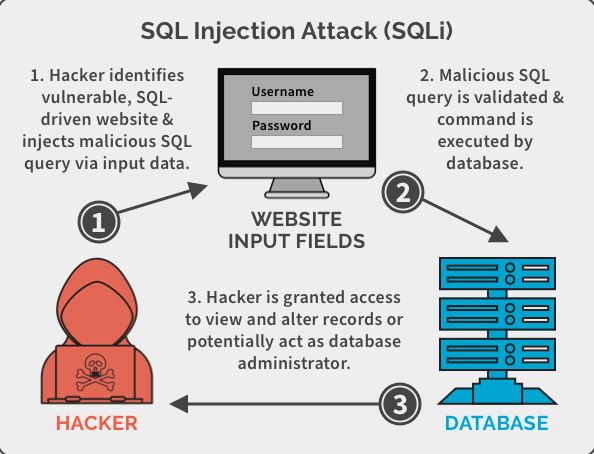
|  |  |
| --- | --- |
| **Threat** | **Category** |
| Hackers attempting to get to the data stored on the site.   * Change data * Delete data * Add fake or wrong data | External\* |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply is down * Cable is failed to link | Internal |
| Denial of service attacks to bring the service down.   * Flooding with traffic * Sending information that triggers a crash | External |
| Data destruction by any means such as a user deleting a file.   * Delete data * Move data to a separate folder * Format the hard drive | Internal\* |
| Misuse of information by internal staff.   * Copy confidential work data * Access to personal data | Internal\* |
| Power problems so site is down.   * Power cut off * Power supply is down * Maintenance | External |
| Overloaded site so response is slow.   * Network problem * Data provider issue * Maintenance | External |
| Customers falsifying information to avoid payment.   * Provide wrong data * Missing payment | External |
| Incorrect information such as wrong prices so customers pay too little.   * Losing income | Internal |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.   * Low customers’ satisfaction * Negative feedback | Internal |
| Major disaster so site is down.   * Earthquake, bushfire, tsunami, flood etc. * Terrorist | External\* |

### 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>





**Comment:** SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

## 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 and software areas include:

* **Booking of test.** This will be time-critical and the information provided will need to be kept secure. The system should be easy-to-use and efficient so bookings can be made as quickly and as accurately as possible.
* **Automatic test download.** The automatic request must be sent and the correct test downloaded within the appropriate time frame.
* **ISDN link to obtain test.** Given the time-critical factor, the system cannot be down for more than one hour.
* **Test data.** Data will need to be kept secure so that students do not know which questions will be asked.
* **Accounting processes.** The system must ensure that all student monies are received and control the tests that are charged for by the vendor.

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

* **Security Threat:** Security threat is defined as a risk that which can potentially harm computer systems and organization. In the cause, students will pay by credit card or bring cash to the centre, so their information about credit card under threat. Additionally, the centre will keep stocks of these certificates for each vendor. Sot the centre have ensure that those information security.
* **ISDN Threat:** ISDN is set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. In this cause, if there is something wrong with the telephone network system, then the students cannot have the text.
* **Physical Threats:** a physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

1. **Internal:** The threats include fire, unstable power supply humidity in the rooms housing the hardware
2. **External:** These threats include Lightning, floods, and earthquakes.
3. **Human:** These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

* **Non-physical threats:** loss or corruption of system data, disrupt business operations that rely on computer systems, loss of sensitive information, illegal actives, Virus, Trojans, Worms.

## 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 4: 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 locations | 5 | 4 |
| Hardware problems that stop system operating | 1. The quality of hardware 2. Fault tolerant system | 4 | 5 |
| Credit card fraud. With the short time frame the student could be tested before any credit card discrepancy was identified. | 1. Verify identity before taking exam 2. Insurance to cover fraud 3. Change business processes to only take cash | 4 | 5 |
| Student not turning up and exam lapses so $50 is lost. | 1. Charge a cancellation fee at time of booking 2. Set up a system to try to reuse exam before expiry | 1 | 2 |
| ISDN links broken delaying download of exams | Alternate Links | 5 | 5 |
| Hackers who may try to access test data or student data | 1. Encryption 2. Firewalls 3. Monitoring network | 1 | 5 |
| Internal unauthorised access to test data or student data | 1. Encryption 2. Firewalls 3. Monitoring network | 3 | 3 |
| Theft or misappropriation of test certificates | Secure system for certificates | 4 | 5 |

## 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.

### 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?

* Clustered systems
* Allows system to continue working even if a hard disk fails
* Additional disks or disk subsystems
* Improved performance

1. Threats to be safeguarded against

* Failure to eject hard drives and storage devices before properly turning them off or disconnecting them
* Improper system shutdowns
* Sudden power outages
* Hard drive failures, bad disk sectors, and other hardware-related problems

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

* Orders placed on the web $100,000 per day
* The backup tapes could be on average 12 hours (loss for this time= $50.000)
* 50% would go elsewhere if the system is down
* The cost of a RAID system would be in the region of $12,000

1. How RAID supports the business?

* Managing files in a more efficient way
* Improve your business productivity and storage management
* Disk striping, a technique that mirrors data over multiple disk drives, allowing you to read or write to more than one disk at the same time
* 24/7 operation

**Comment:** It’s important to note that RAID provides protection against faulty hard drives; however, RAID is not an insurance policy against other potential computing issues that may arise. For example, RAID does not protect your business against data loss that can occur due to malware, accidental file deletions, or natural disasters. RAID is simply a fail-safe for hard drive failures. RAID is not a substitute for proper backup practices.

All RAID levels apart from RAID 0 offer single-drive failure protection, while RAID 6 can be configured to stay online even if two disks fail simultaneously.

## 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.

Some computer viruses have a performance impact by slowing down the network (sometimes to a level causing loss of view); others might corrupt data and programs impacting the availability of the server / station. Removing the malware infection is another important factor that impacts the continuity of the process control system. Depending on the type of malware this can be done with special utility programs provided by the anti-virus software provider, or it may require a full restore from back-up. In all cases the cost in time and resources of a malware infection is high, even when production continuity has not been impacted.

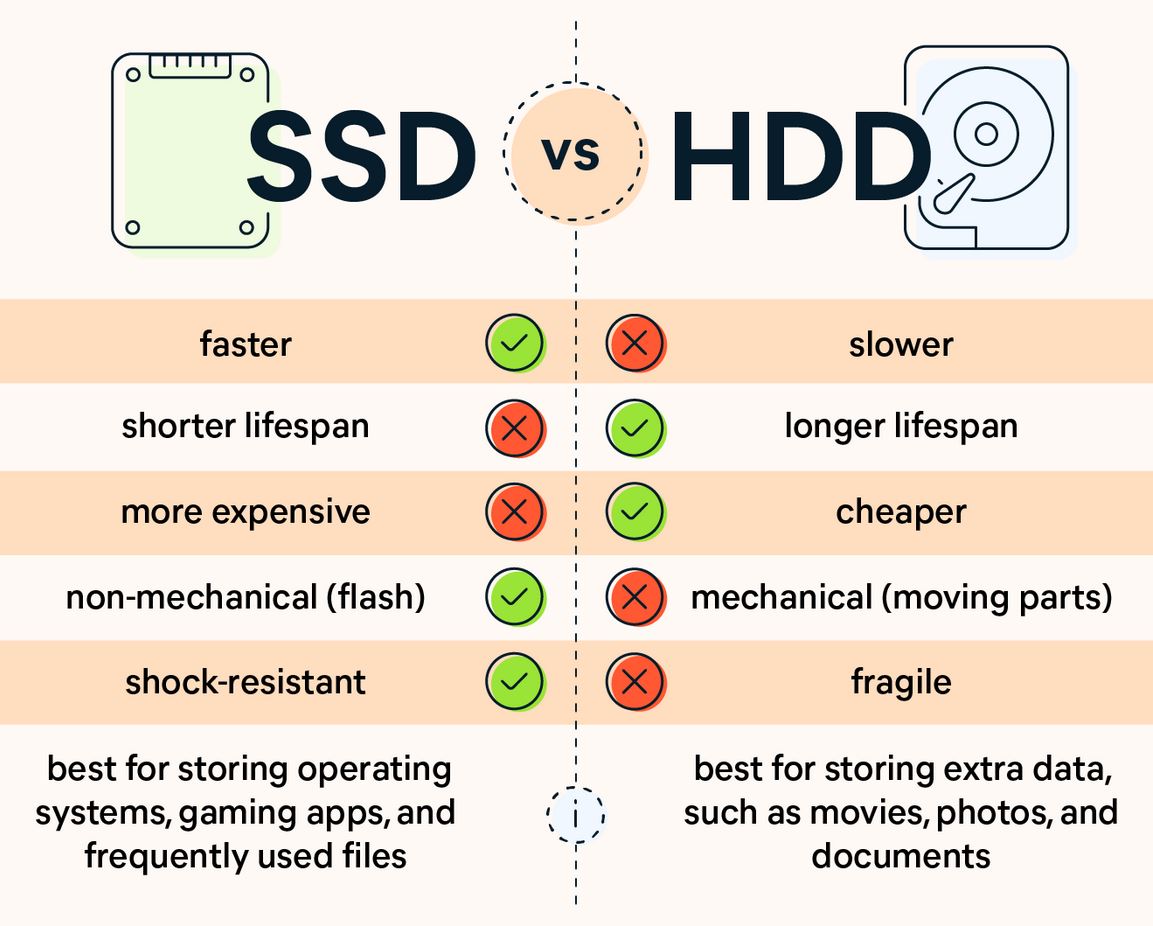
For the correct operation of procedures against computer viruses it is necessary to take into account the following:

- Use a more secure operating system. Computer viruses often target Windows computers because so many more run on a Windows operating system. An alternative is to run a Linux operating system or Apple’s OSX.

- Install anti-virus software and keep it up to date: it usually prevents the device from known viruses. The anti-virus software on a device must be kept up-to-date so that it can deal with new threats.

- Never open email attachments that contain executable files - files with extensions such as .exe, .com and .vbs. They are capable of doing whatever wrong they have been programmed to do if opened.

- Never open email links that you don’t trust. Treat it as a source that you are not expecting, similar to executable files.

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

**Backup recommendations**

**Backup and Restore** is a component of Microsoft Windows introduced in Windows Vista and included in later versions that allow users to create backups and restore from backups created earlier. It is a replacement of NTBackup, which was included in previous Windows versions.

**Backup procedures**

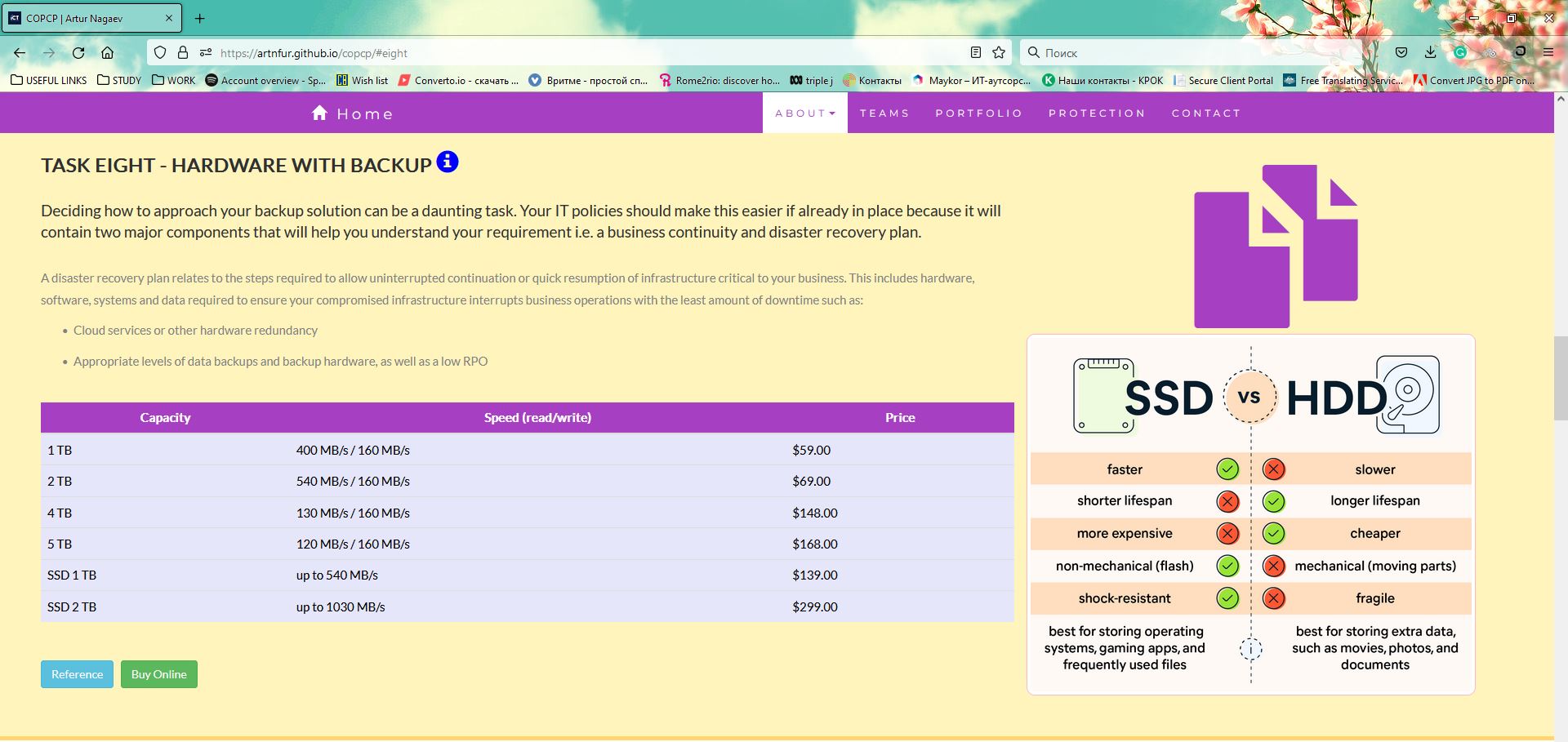
- It is recommended to keep at least 2 or more backup copies of your data and that these should be updated on a regular basis. Storing these backups in different physical locations will help ensure you have at least a backup copy elsewhere should disaster strike one of your locations.

Experts recommend the 3-2-1 rule for backup: three copies of your data, two local (on different devices) and one off-site. For most people, this means the original data on your computer, a backup on an external hard drive, and another on a cloud backup service.

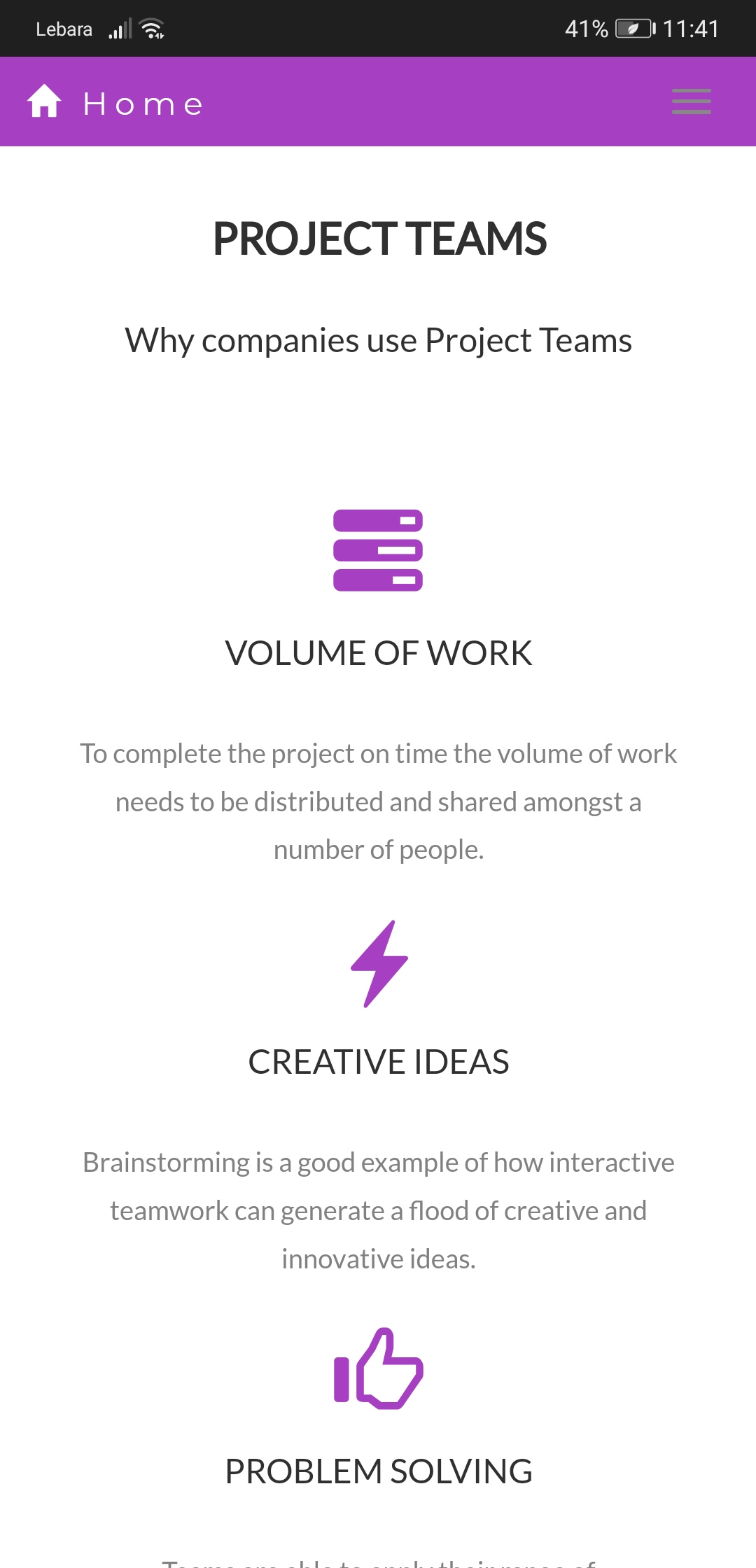
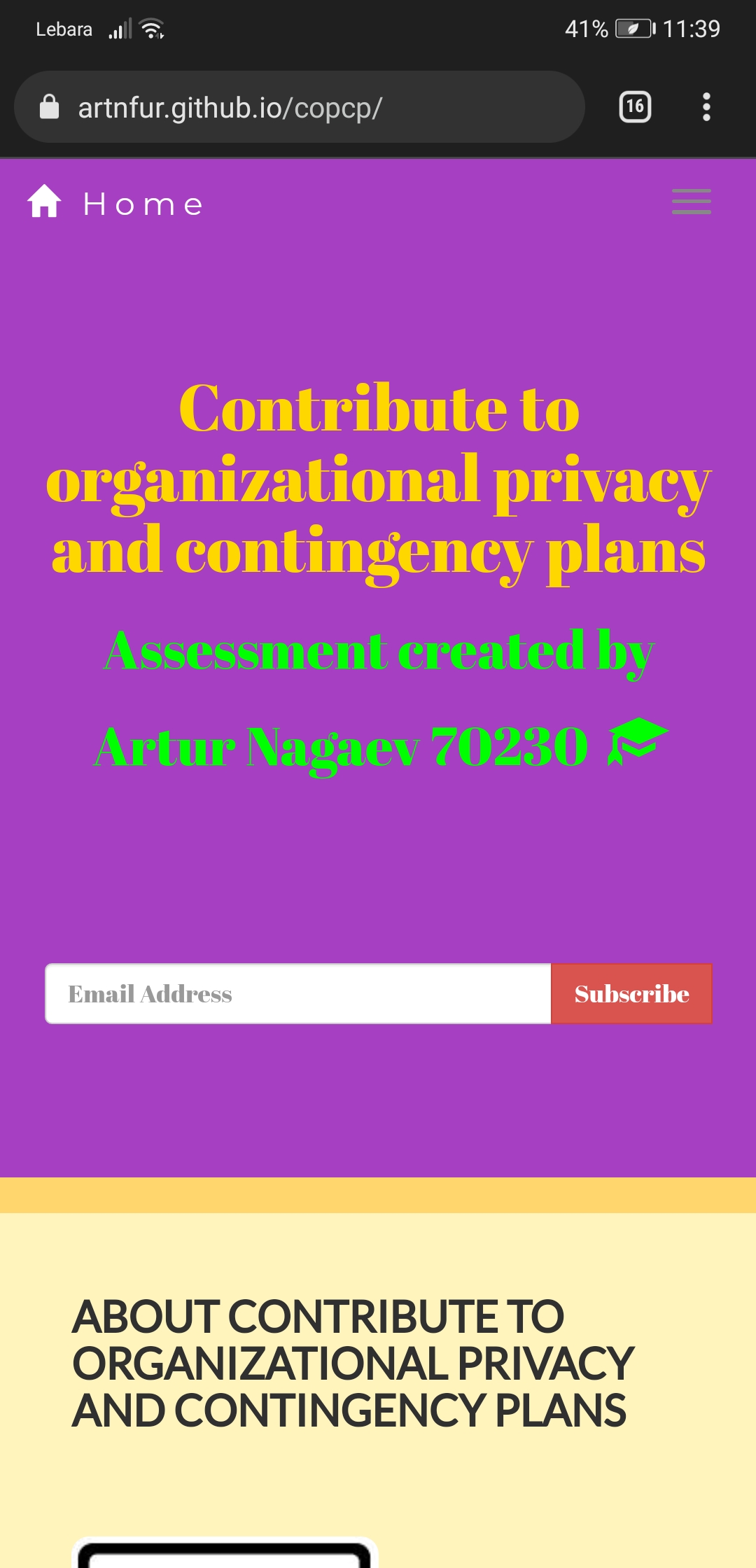
**Forming a Backup Strategy: 4 Steps to Follow**

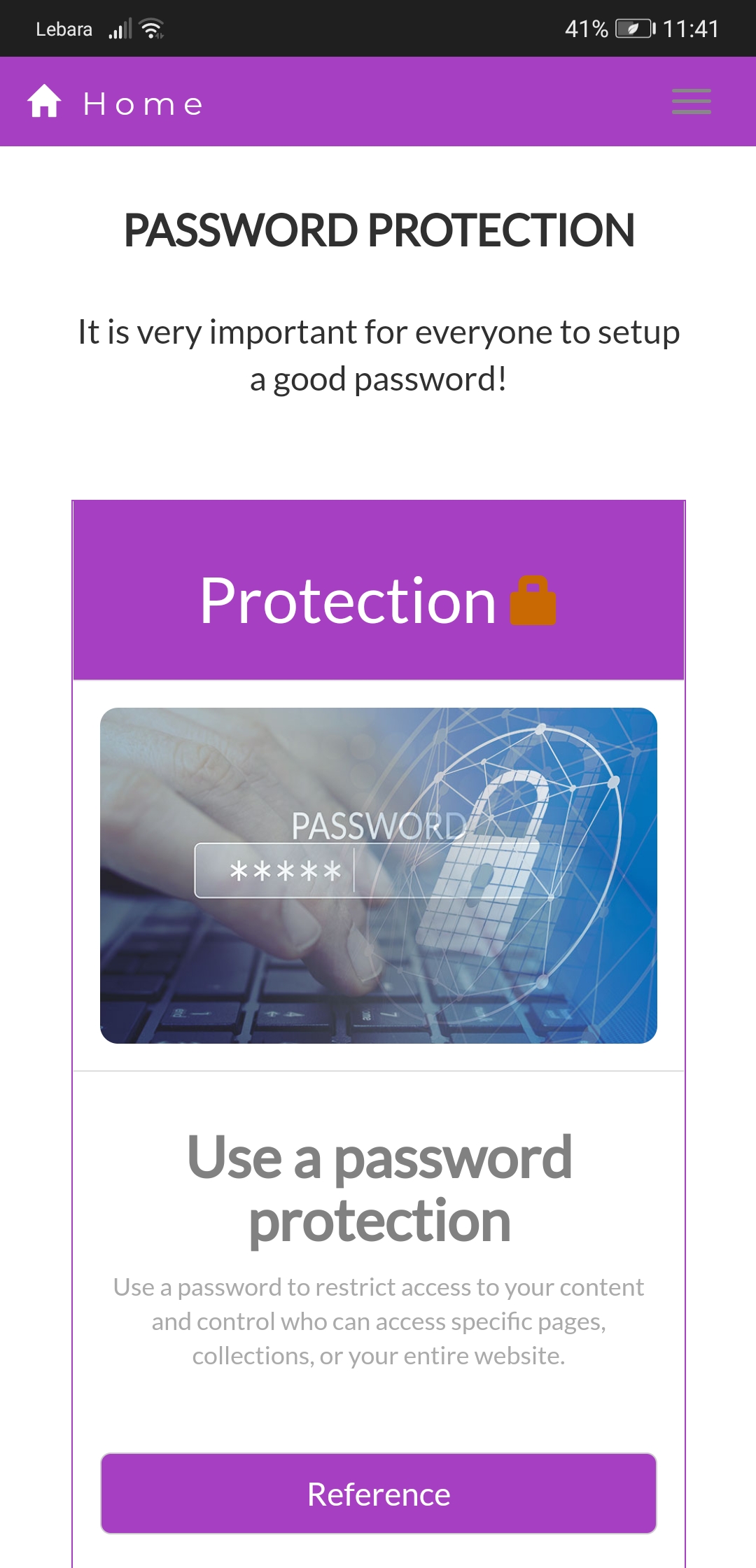
* Determine what data has to be backed up.
* Determine how often data has to be backed up.
* Identify and implement a suitable backup and recovery solution.
* Test and Monitor your backup system.

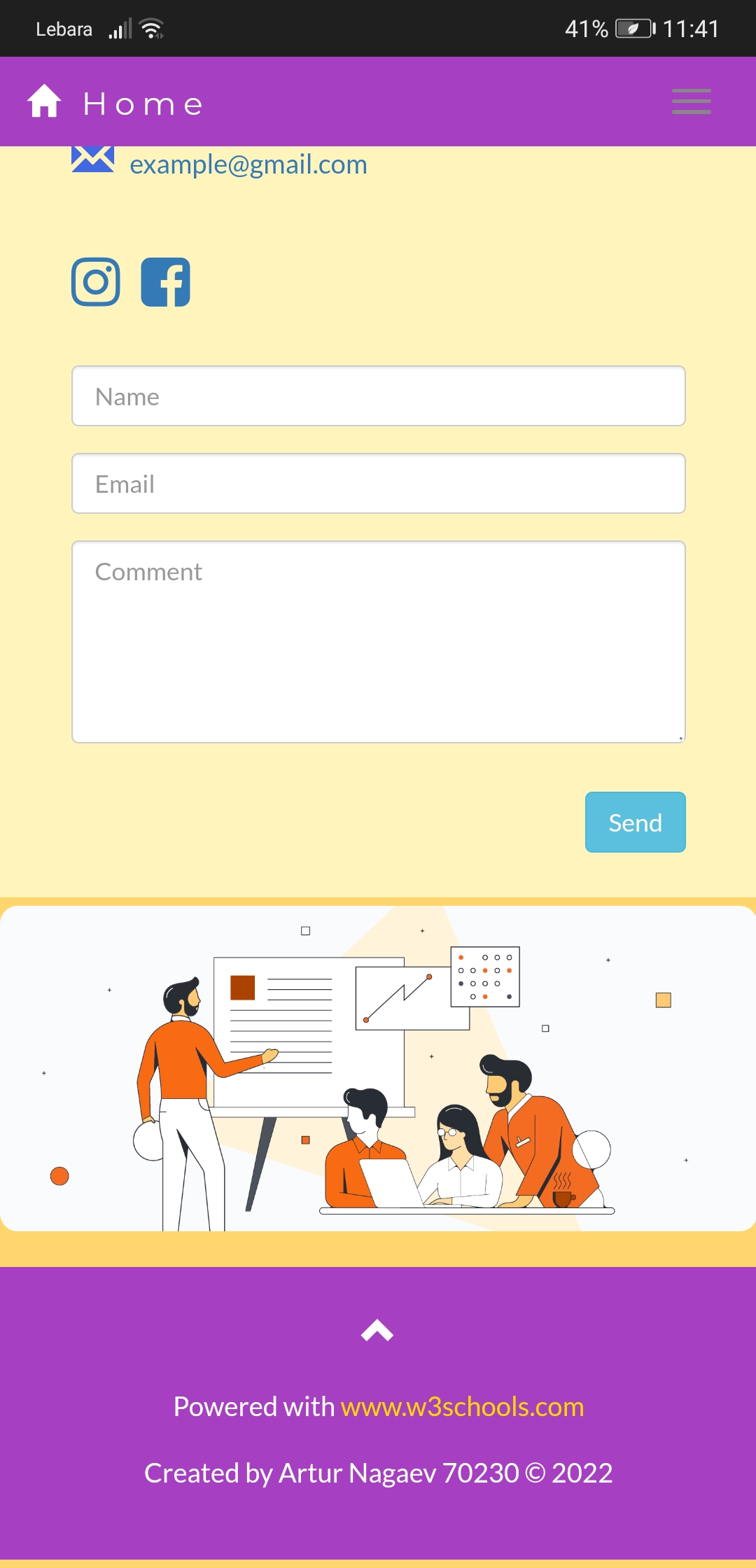
|  |  |  |
| --- | --- | --- |
| **Capacity** | **Speed (read/write)** | **Price** |
| 1 TB | 400 MB/s / 160 MB/s | $59.00 |
| 2 TB | 540 MB/s / 160 MB/s | $69.00 |
| 4 TB | 130 MB/s / 160 MB/s | $148.00 |
| 5 TB | 120 MB/s / 160 MB/s | $168.00 |
| SSD 1 TB | up to 540 MB/s | $139.00 |
| SSD 2 TB | up to 1030 MB/s | $299.00 |



**You can find my website via link**: <https://artnfur.github.io/copcp/>







## Index

B

backup 5, 13

backup and restore 13

C

critical 3, 4, 5, 6, 8, 9, 11

D

duration 2

I

increased 13

ISDN threat 9

N

new viruses 13

non-physical threats 10

O

organisation 3, 6, 8, 9, 13

P

physical threats 10

privacy 2

R

RAID 11

recovery 10, 13

S

security threat 9

software purchases 13

SQL injection 8

T

threats 7, 9

V

virus 12, 13

virus protection 13