Wells International College

[Company name]  [Company address]

Contribute to Organizational Privacy and Contingency Plans

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Tomohiro Matsuyama | ID | 70351 |

# 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:

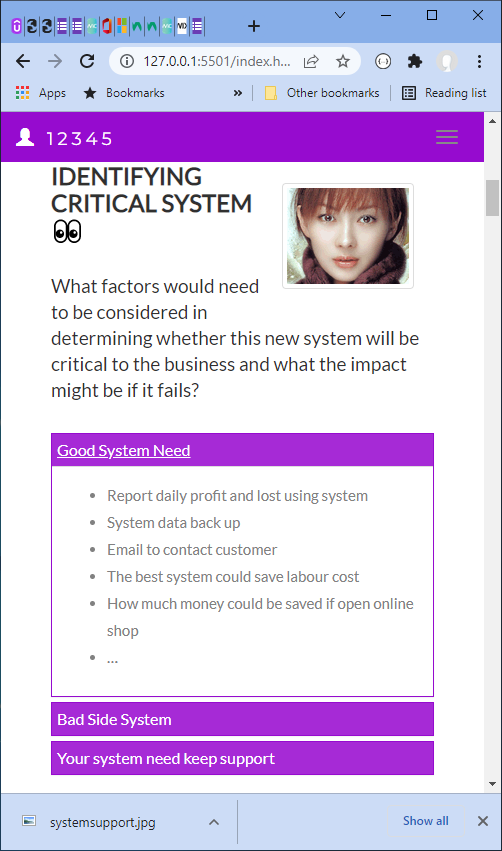
Trainer will set the duration of the assessment.

## 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:

* Report daily profit and lost using system
* System data back up
* Email to contact customer
* The best system could save labour cost
* How much money could be saved if open online shop
* Efficient to inventory management
* Easy to tack sales and make a report
* Possible to send items to all over the world
* Greater selection

Bad side:

* if fail down, you will be lost customer
* need easier to contact to customer
* could be big cost
* Increase risk of fraud
* Longer wait time than walk in shopping
* Returns can be complicated
* Not opportunity to touch/feel items

URL:

Comment: There are pros and cons to online shopping business, as above;

In order to reduce a risk of using website for online shopping, risk reduction management is essential to be in place. As an example of it, contingency plan can play a vital role in responding to a potential future incident.

Please check my website to know about more a contingency plan.

<https://wellsjohn220.github.io/copcp>

or (old):

<https://johnyeewarwick.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.

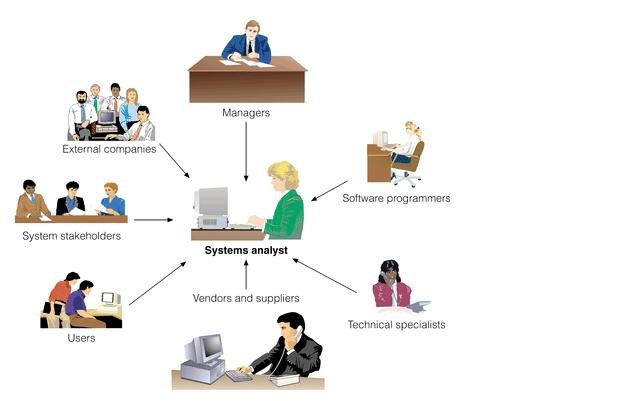
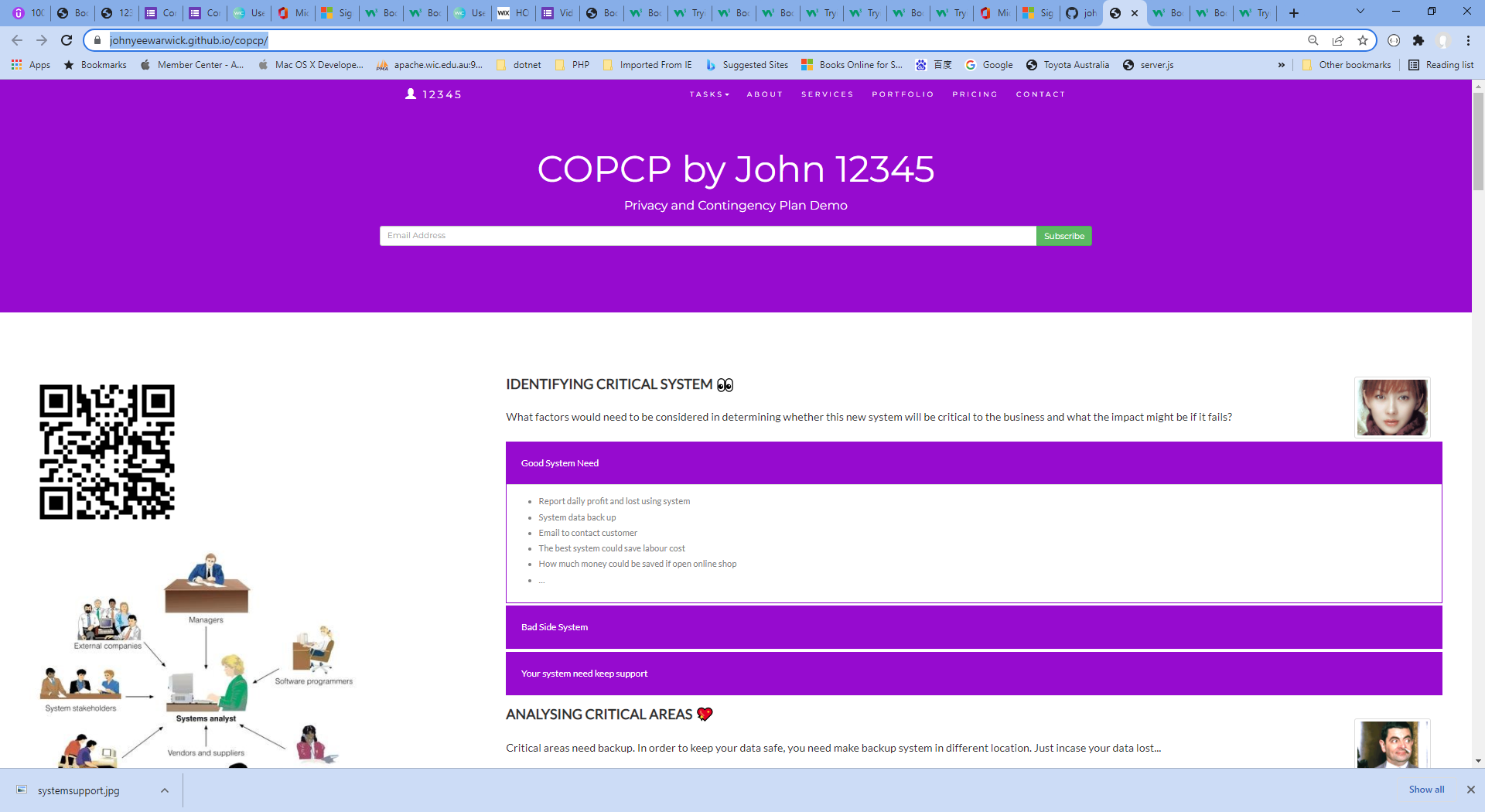


Table 1: critical areas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Update corporate data files** | **Create own data files** | **Create shared documents** | **Create own temporary documents** |
| **From source documents** | 70% | 50% | 20% | 20% |
| **From other data files** | 10% |  |  |  |
| **From irrecoverable sources such a telephone calls** | 60% | 50% | 30% | 30% |
| **Developed at the workstation such as report writing** | 0 | 50% | 50% | 20% |
| **Other—specify** | 0 | 50% | 50% | 0 |



#### 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
* …

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
* …

## 

You comment:

Backups can be corrupt for several reasons. Old media can get damaged or corrupted through poor handling or simply through age. Readable backups may not have application-consistent data, so even though you restore files, applications may not come up successfully.

## Scenario 3: determining system criticality

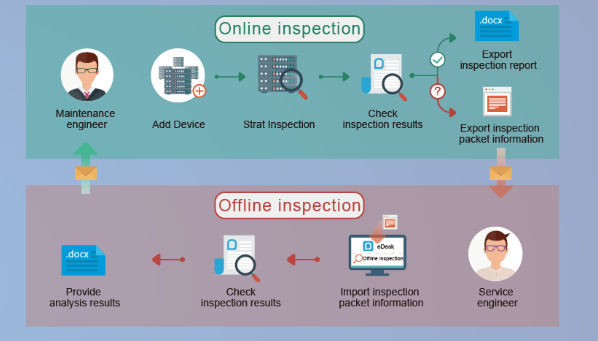
Consider the case study of Urban Wear again. You have the following information about its e-commerce system.

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 |  |  |
| **Impact on profitability** | X |  |  |
| **Impact on customer or supplier relations** | 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:

…

1. lost opportunity

A single online purchase might not hurt. But what if hundreds or thousands of online buyers are affected? Profits can take a big hit. In addition, several bad experiences can discourage customers from making repeat purchases. That's why the impact of system downtime can be disastrous for some companies (like most e-commerce websites) the moment it strikes.

1. lost productivity

Some network services are needed by employees and third parties in order to do their work. When those services become unavailable, the affected parties won't be able complete certain tasks. This can have a domino effect that can bring down overall productivity.

1. eroded confidence

Even trading partners with long established business relationships with you can lose their patience if your downtimes start affecting them significantly as well. Any delay at your end due to an unavailable service can also cause delays to other companies along the supply chain. They too can suffer the same consequences outlined in this article.

1. Damaged reputation

To make things worse, broken promises can now have serious repercussions, other than the financial type. Many disgruntled customers or employees of trading partners are quick to vent their frustrations on social media. In just a few minutes, word about your "lengthy" downtime can reach across the globe.

**How to prevent downtime**

One way to minimize network service downtime is by setting up redundant systems and deploying high availability solutions

#### Task 3:

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

A high availability solution is to ensure system uptime even in the event of a failure. Redundancy, on the other hand, is the use of additional software or hardware to be used as backup in the event that the main software or hardware fails. To deploy both systems and solutions can reduce a risk of using online shopping.

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.
* …

## 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\*  Phishing |
| Hardware failures that stop the site operating.   * Hard disk broken * Power supply down * Cable is failed to link | Internal threads |
| Denial of service attacks to bring the service down.  ... | Ex  A distributed denial-of-service (DDoS) attack |
| Data destruction by any means such as a user deleting a file.  ... | Internal  Threads |
| Misuse of information by internal staff.  ... | Internal  threads |
| Power problems so site is down.  ... | Ex  Power outages |
| Overloaded site so response is slow.  ... | Ex  HTTP Requests Overload |
| Customers falsifying information to avoid payment.  ... | Ex  Payment fraud |
| Incorrect information such as wrong prices so customers pay too little.  ... | Internal threads |
| Incorrect information such as wrong quantity in stock so customers have to wait for delivery.  ... | Internal threads |
| Major disaster so site is down.   * Earthquake, bushfire, terrorist * Flooding | Ex\*  fire or earthquake which renders the system inaccessible. |
|  |  |

#### Task 4:

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

Internal thread

* Incorrect information such as wrong quantity in stock so customers have to wait for delivery.
* Incorrect information such as wrong prices so customers pay too little.
* Misuse of information by internal staff.
* Data destruction by any means such as a user deleting a file
* Hardware failures that stop the site operating.

External thread

* Major disaster so site is down.
* Customers falsifying information to avoid payment.
* Overloaded site so response is slow.
* Power problems so site is down.
* Denial of service attacks to bring the service down.
* Hackers attempting to get to the data stored on the site potential threads
* External thread

Potential thread

1.Account hijacking using dirty dancing in sign-in OAuth-flows

#### 2.Browser-Powered Desync Attacks: A New Frontier in HTTP request smuggling

#### 3.Bypassing .NET Serialization Binders

## 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.

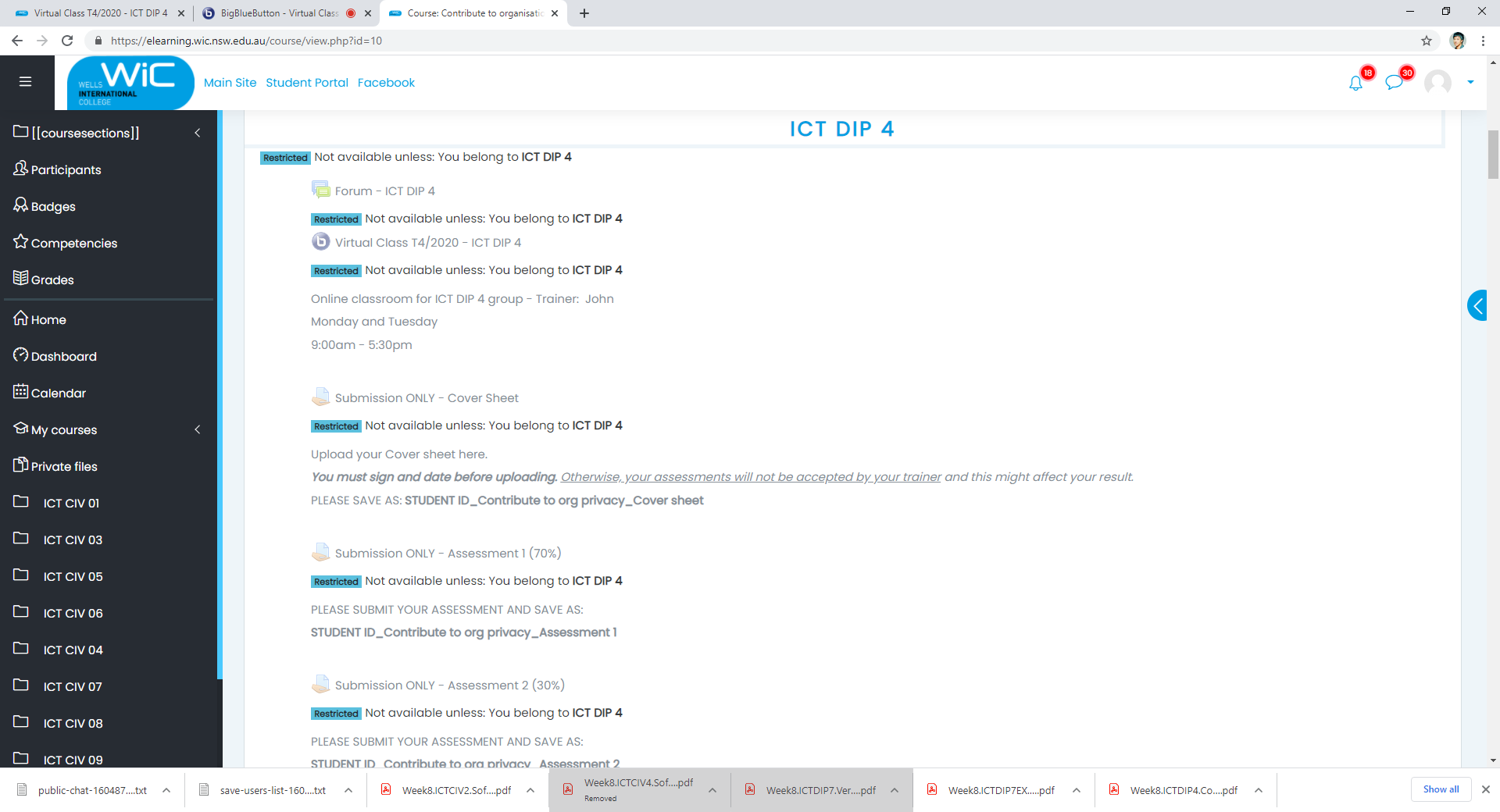
The following are extracts from the business case and other project documentation that has been developed for this project.

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
  + Student credit card information

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

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

Your comment:

Risk analysis is an analytical process undertaken to evaluate system assets and examine their susceptibility to threats has been done above. Through this process we evaluate the possible commercial losses that may result from the loss of these assets. After that, the prevention and recover plan can be in place.

The loss of IT systems could have a major impact on many businesses. Many would come to a standstill in minutes without their critical business systems. Even a small company could get into financial difficulties if it lost its accounting data and did not know who owed it money.

## 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. | Fraud detection software | 4 | 5 |
| Student not turning up and exam lapses so $50 is lost. | Backup system | 3 | 5 |
| ISDN links broken delaying download of exams | An ISDN-PRI test call is also a maintenance procedure concerned with the identification and verification ISDN-PRI user-network interface problems | 2 | 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 | Strong password policy, two factor authentication and Monitoring user activity | 3 | 5 |
| Theft or misappropriation of test certificates | **Deploy data loss prevention (DLP) tools and email gateways** | 3 | 5 |

Comment:

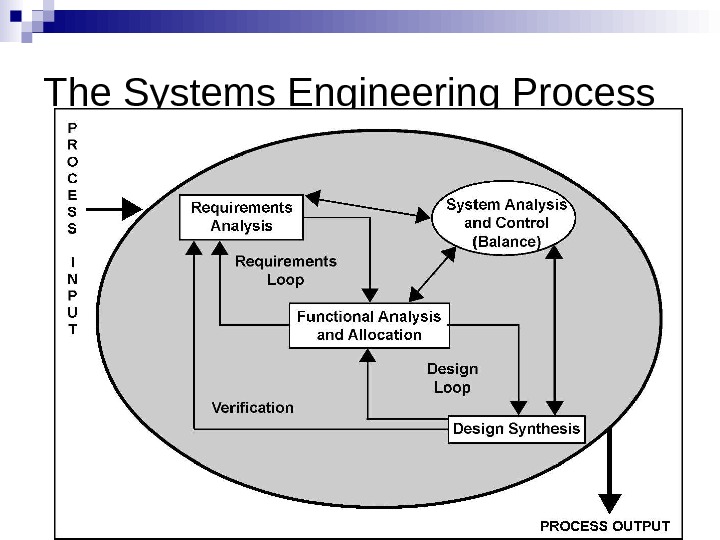
Recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the “system,” the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

* Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
* Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
* Connectivity to a service provider (fiber, cable, wireless, etc.)
* Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
* Data and restoration

Some business applications cannot tolerate any downtime. They utilize dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. This is a very expensive solution that only larger companies can afford. However, there are other solutions available for small to medium sized businesses with critical business applications and data to protect.

## 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.

Comment

A redundant array of independent disks (RAID) is a common system for high-volume data storage at the server level. RAID systems use many small-capacity disk drives to store large amounts of data and to provide increased reliability and redundancy. Such an array appears to the computer as a single logical unit consisting of multiple disk drives.

RAID storage can be done in a number of ways. Some RAID types emphasize performance, others reliability, fault tolerance or error correction. Which type you choose depends on what you're trying to accomplish.

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:

RAID isn't the only way to protect large amounts of data, but regular backups and mirroring software are slower and often require shutting down the system if a drive fails.

Even if the disk doesn't crash the server, information technology workers would still need to shut down the servers to replace the drive. RAID instead rebuilds data from the remaining drives using mirrored or parity information, without requiring a shutdown.

The three most common RAID implementations are Levels 0, 3 and 5.

RAID Level 0, data striping, is the most basic model. On a normal hard drive, data is stored on consecutive sectors of the same disk. RAID 0 uses a minimum of two disk drives and divides data into blocks that range from 512 bytes to several megabytes, which are written alternately to the disks. Segment 1 is written to Disk 1, Segment 2 to Disk 2, and so on. When the system reaches the final drive in the array, it writes to the next available segment of Drive 1, and so forth.

Striping the data distributes the I/O load evenly across all the drives. And since drives can be written to or read from simultaneously, performance increases noticeably. But there's no data protection. If a disk fails, data is lost. RAID 0 isn't for mission-critical environments, but it's well suited to applications such as video production and editing or image editing.

RAID Level 3 includes data striping, but it also assigns one drive to store parity information. This provides some fault tolerance and is especially useful in data-intensive or single-user environments for accessing long sequential records. RAID 3 doesn't overlap I/O, and it requires synchronized-spindle drives to prevent performance degradation with short records.

RAID Level 5 is similar to Level 0, but instead of dividing data into blocks, it stripes the bits of each byte across multiple disks. This byte-striping adds overhead, but if a drive fails, it can be replaced and the data reconstructed from parity and error-correcting codes. RAID 5 overlaps all read/write operations. It requires three to five disks for the array and is best suited to multiuser systems that don't need critical performance or that do few write operations.

## 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. ...

It’s vital that you keep your PC’s protection up to date, otherwise newer threats may be able to slip past your defences. Thankfully, in most cases, updating can be handled automatically. Updating your antivirus software doesn’t mean shelling out for a whole new software package. Most updates only involve installing the latest virus database definitions, and this can be a reasonably quick process.

Your security software should be set to check for updates at least once a day; this will already be the default setting for most current security programs, although it’s worth investigating your program’s settings to make sure this is the case. If you’re in any doubt, and think that there might be a virus on your computer, then most security software suites or antivirus programs allow you to do an on-the-spot update to check for the latest threats.

Your security software gives real-time protection against threats as they emerge, but regular system scans are vital. Most security suites are configured to perform a scan once a week.You can usually customise the schedule, although scanning your entire PC every day is probably overkill, while leaving more than a week between scans is not safe. Antivirus programs often offer two types of scan: a ‘quick’ scan and a ‘deep’ or ‘full’ scan. Set your software to do a full scan once a week. You can also do a further manual ‘quick’ scan any time you choose, although this is only usually necessary if your PC is exhibiting suspicious behaviour.

#### 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**

Antivirus is a type of computer program that's designed to seek out and remove computer viruses that have infected your computer. They can also block your system from getting infected with new viruses. There are antivirus programs available for every operating system, including Windows, Mac OS, Android, iPhone, and even Linux.

For the most part, even if you're using an Android or a Windows computer, modern systems are already fairly well protected. For example, Windows 10 comes with [Windows Defender](https://www.lifewire.com/protect-your-pc-with-windows-defender-3507028), which includes a firewall and an antivirus component. However, Windows Defender isn't a perfect solution.

[Antivirus](https://www.lifewire.com/antivirus-4781468)

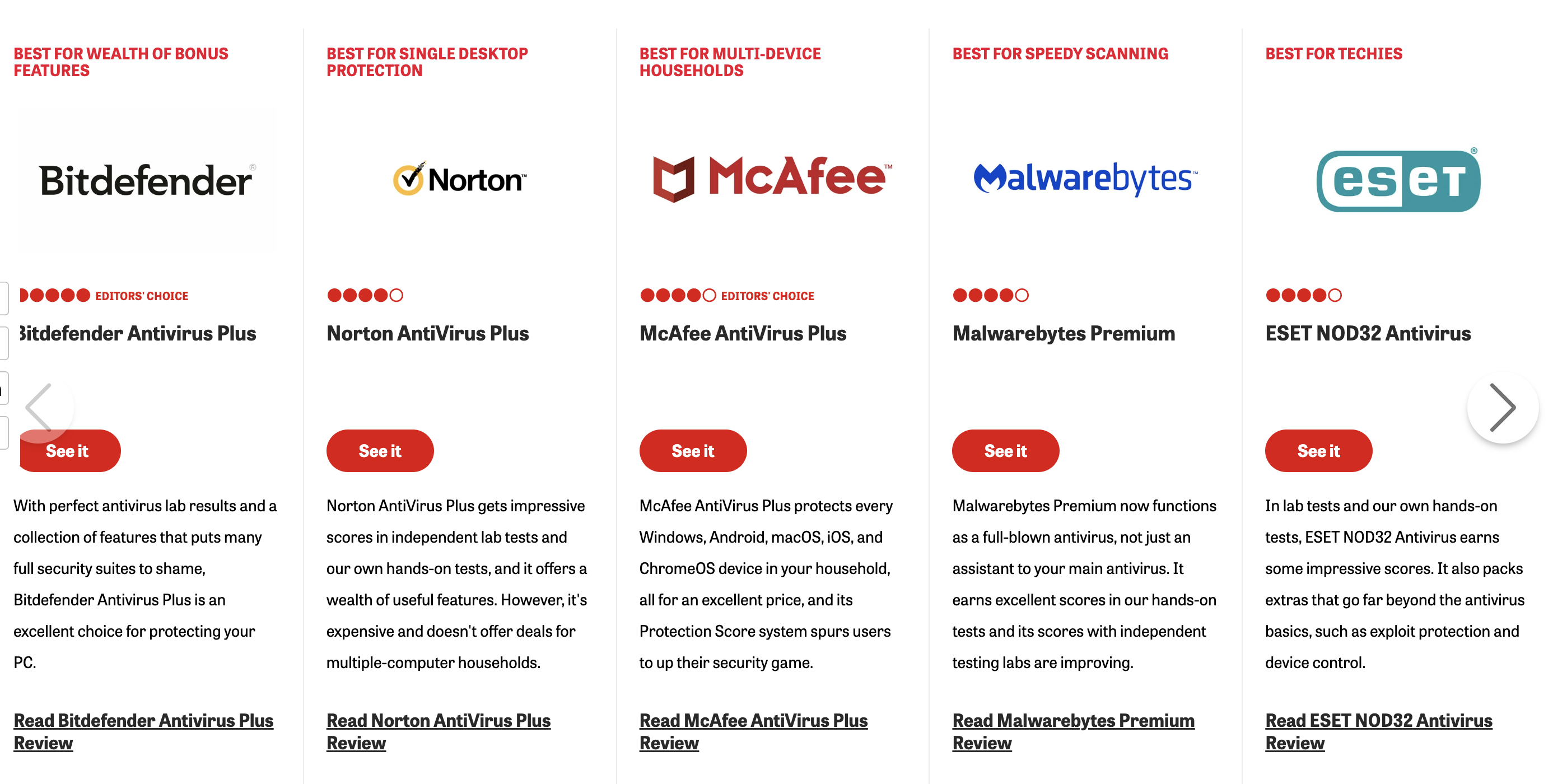
The following actions on your part can still put your computer at risk if you don't install antivirus software:

* Clicking on email phishing links.
* Downloading free software from unknown sources.
* Using peer-to-peer file sharing software.
* Clicking on malicious social media links.

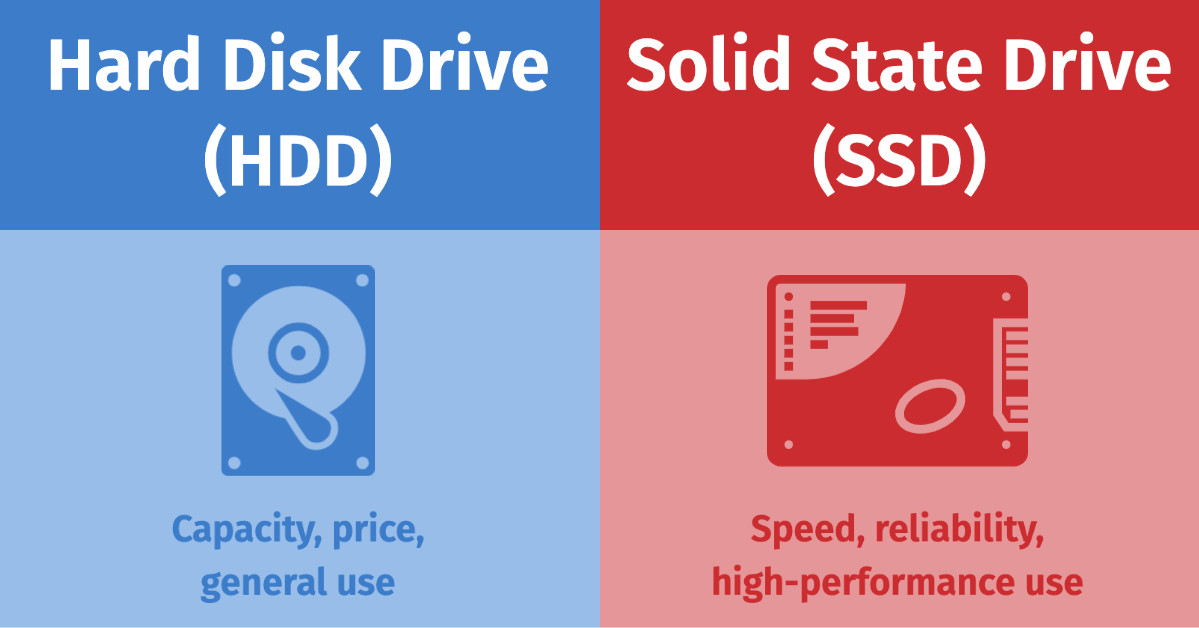
There are two main functions of antivirus software, blocking viruses from infecting your computer from the internet, but also protecting your computer from your own mistakes.

All you need to do is choose from any of the top free antivirus apps available for Windows 10. If you're using an Android device, there are plenty of great [free antivirus apps](https://www.lifewire.com/best-free-antivirus-android-4151993) for Android as well.

These antivirus apps protect you from every source of malware. Everything from Trojan viruses and zero-day exploits to computer worms and ransomware. Install one immediately and make sure to schedule a scan regularly.



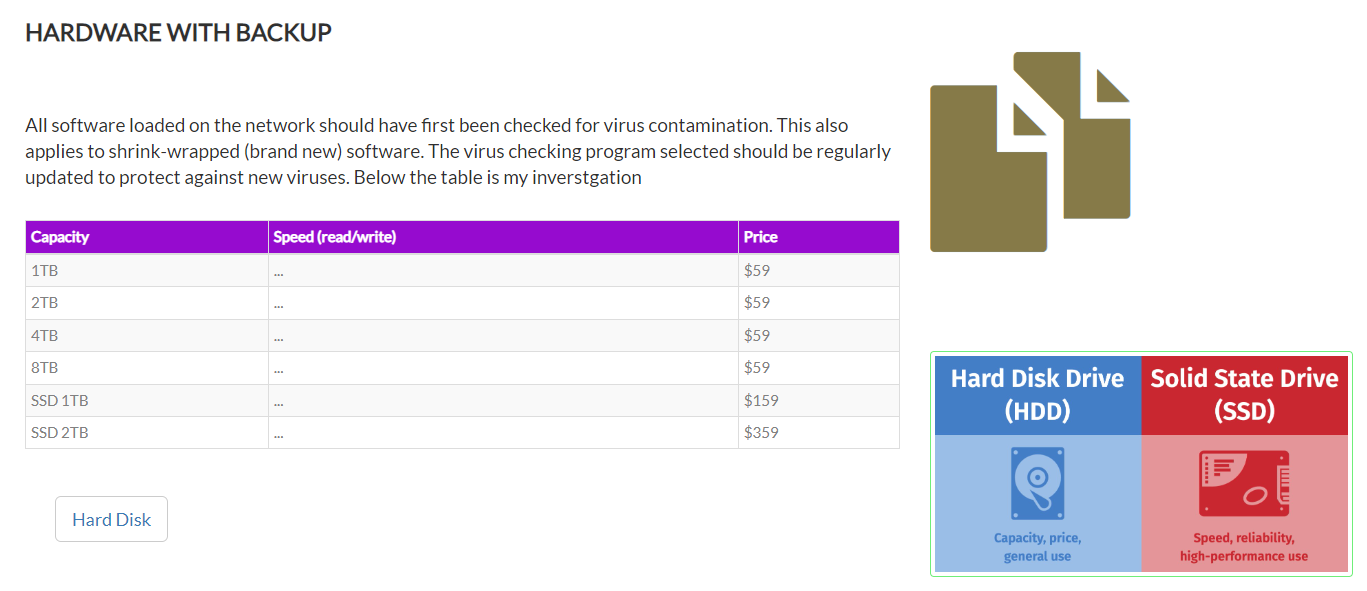
1. You will need to recommend hardware or software purchases to improve backup and recovery in the event of a disaster.

**Hardware recommendations**

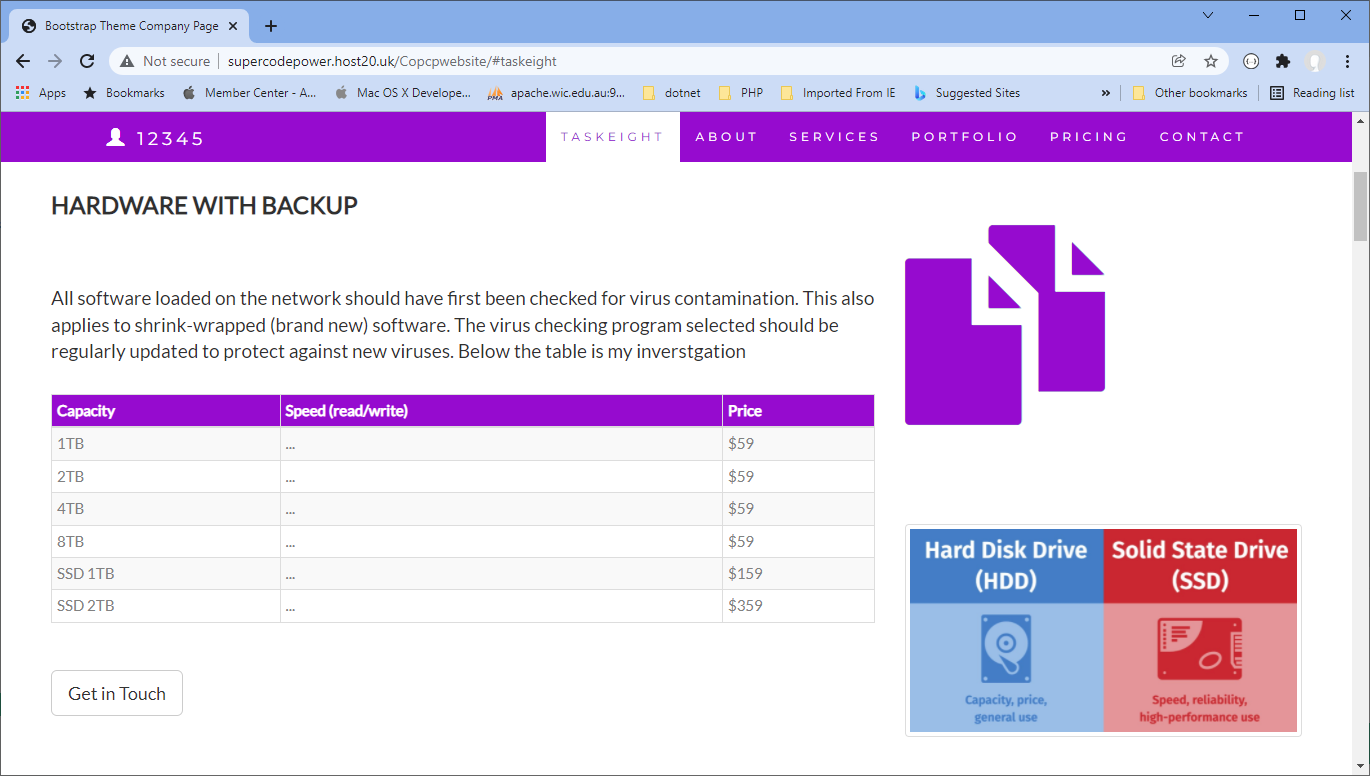
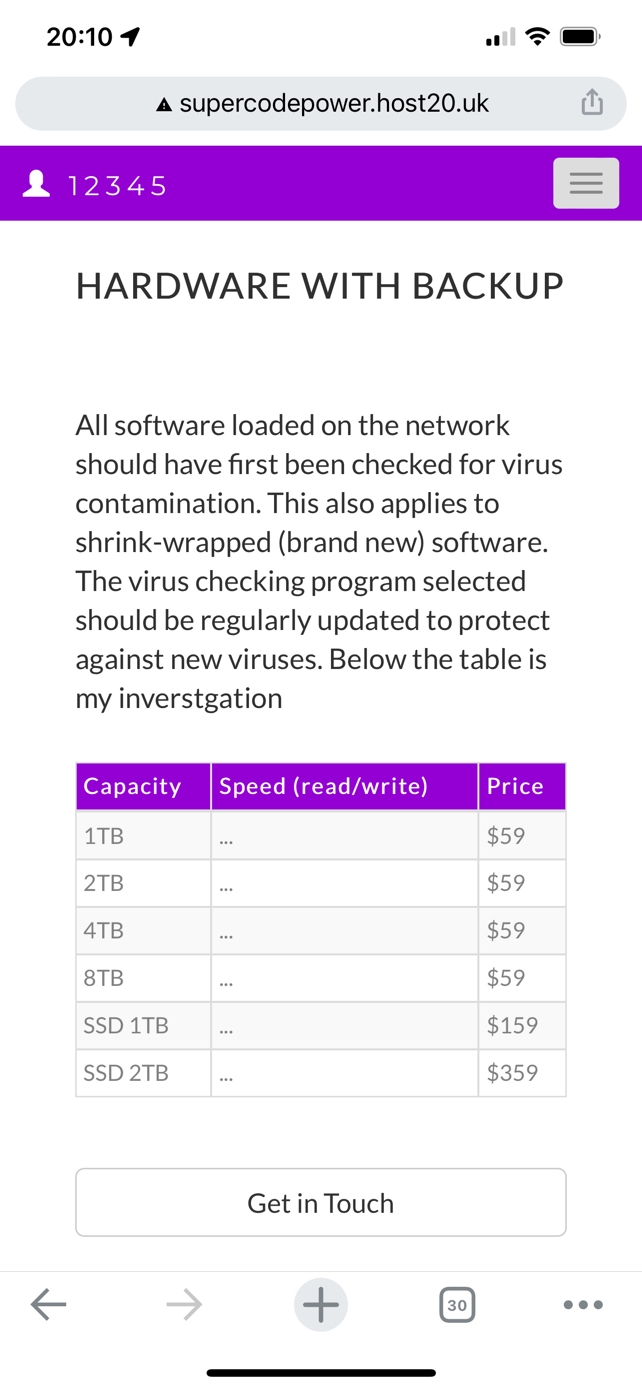
The current tape unit is too slow and does not have the capacity to store a full back up on a single tape. Typical hardware specifications and costs are:

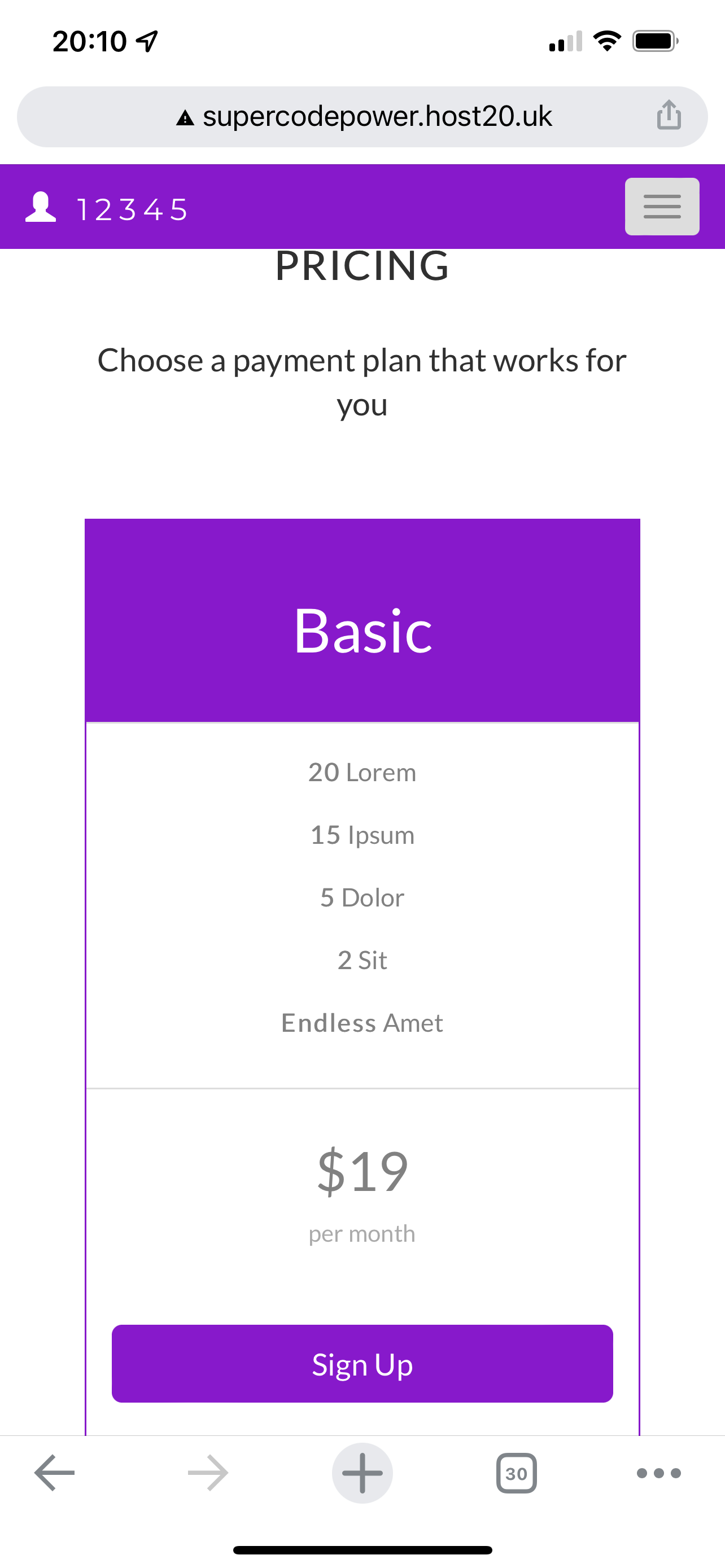
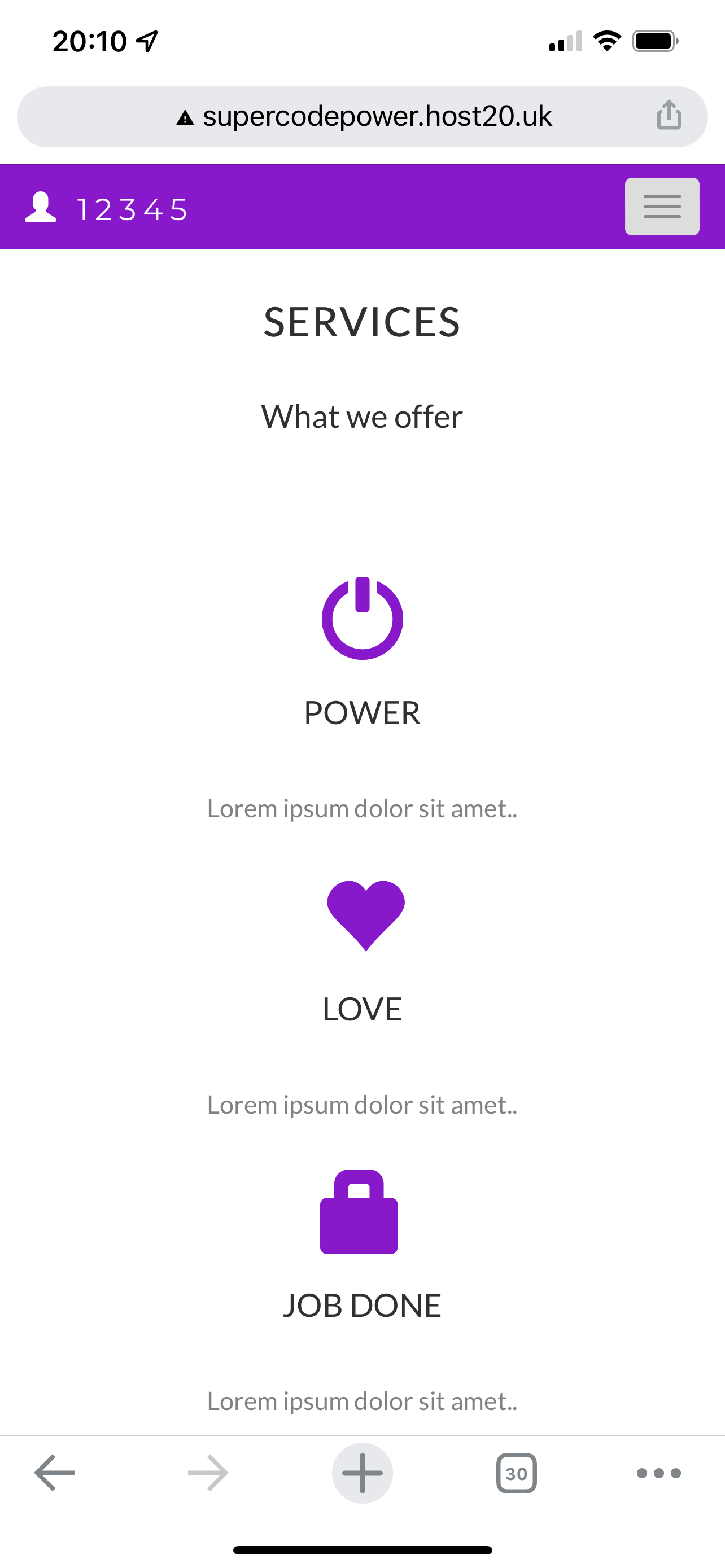
|  |  |  |
| --- | --- | --- |
| Capacity | Speed(read/write) | Price |
| 1TB | read/write speed of 147 MB/s | $59 |
| 2TB | read/write speeds are above average at 190 MB/s | $79 |
| 4TB | a read speed measuring 145MB/s and a write speed of 153MB/s | $145 |
| 8TB | 72.17MB/s read and 109.08MB/s write | $256 |
| SSD 1TB | Read speed 3,500 MBps max. Write speed 2,500 MBps max. | A$298 |
| SSD 2TB | About 7,080 mb/s read and 5,249 mb/s write average | $359 |

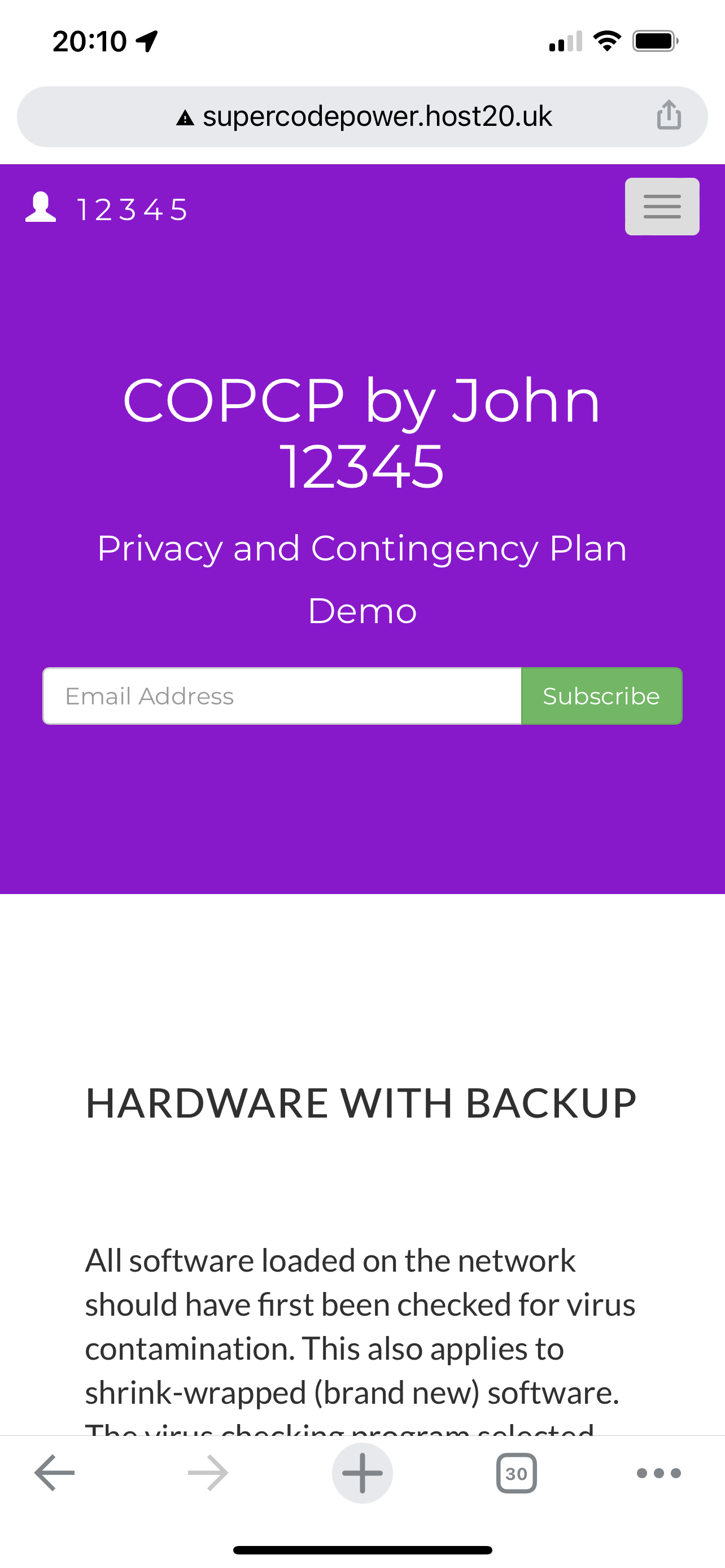
<https://wellsjohn220.github.io/copcp/#taskeight>



Below these is my web contents support.







<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