Name: …….

Cyber security

Some background

Cyber attack is big business both for the criminals and for those trying to stop it

- An example of a threat: The labour party social media attack November 2019
- Q: What attack methods were used here?
- So how serious is it? : attacks on BRITISH BUSINESSES 2019
- 11 day rule: After a major IT failure, you may have as little as 11 days before the operating capacity of your business falls to 10% of its original value. Very few organisation can come back from this level of failure
- Imagine this for AMAZON!!

Useful links

- https://digital.nhs.uk/services/data-security-centre/cyber-security-glossary
- https://cybersecurityventures.com/cybersecurity-glossary/
- https://www.cybrary.it/glossary/

Why is it happening?

Individuals and Organisations must try to

- MAKE information and data Available
- BUT keep information and data secure
- AND MAINTAIN the integrity of the information and data
- Because that data is valuable
- and
- Because if they don't, there are a number of consequences

Name: …….

Q1. Consequences

Consequences can be direct or indirect

DEFIne

Direct consequences

Indirect consequences

Make a list of possible direct and indirect consequences of NOT protecting your organisation from cyber threats

Direct consequences

Indirect consequences

Name: …….

Q2. Assets – what do we need to protect?

Assets are things your organisation has which it would need in order to operate. Therefore these are things you would need to protect these assets.

Here is a list of 6 areas of assets to consider for any organisation which they would need to protect from cyber threats

Asset	Rank (1-6)
Software	
Hardware	
Buildings	
Data	
People	
Communications	

Rank these from 1 (most important to protect to 6 (least important).

In the space below write a statement explaining why you ranked the items in the order you did.

Name: …….

Q3. Key terms in cybersecurity

The following is a list of SOME of the key terms used in cyber security.

Using the internet, find a definition of each key term and write it in the space provided

Account lockout	
Anti-malware Software	
Cyber criminal	
Disaster recovery plan	
Encryption	
Ethical hacking	
Firewall	
Hacker	
Hacktivist	
Honeypot	
Integrity of data	
Malware	
Penetration testing	
Phishing	
Risk analysis	
Sandboxing	
Scammer	
Social engineering	
Spyware	
Virus	

Name: …….

Q4 Spot the weaknesses

What threats are there to organisations and businesses who use networks or the internet?

Remember :– the threat may no always come from outside or be obvious!

Make a list of all the possible threats to an organisation in the space below.

Name: …….

Q5 Defending your system

There are 3 lines of defence for organisations and their systems

- Prevent (stop something from happening)
- Detect (find out that something has happened)
- Recover (deal with the outcome of a cyber attack you did not prevent or detect until it was too late!)

For each of the above lines, list as many possible methods which a business organisation could use as you can

PREVENT	**DETECT**	**RECOVER**

Name: …….

Q5 Essay 44601 (based on 1.3.2 data base question)

Write an answer to the following question

A bank needs to ensure the data stored in its database is accurate and secure at all times including when customers deposit or withdraw funds.

Discuss how the bank can ensure the accuracy of its data and the importance of doing so.

Point – this is not about sending out questionnaires to customers asking them to check stuff!!

You need to think about the need to provide security for the bank's data. Consider what you need to protect and how you might do this. You will also need to consider the legal reasons why you would have to do this.