# Network Security threats and vulnerabilities task

## Scenario:

You are a cyber security consultant.

A small company with 54 employees that create and sell smart fitness tracking clothing and accessories.

They are situated in a small industrial estate. They have the following departments:

Sales

Management: general and human resources

Manufacturing

Purchasing and Finance

Delivery

Site installation for POS displays and demos

Sales have been good as an influx of demand happened as more people started to exercise outside of a gym, as a result they are hiring another 10 employees.

Their IT systems consist of a server, several PCs, a couple of printers and a consumer wireless router connected to the internet. A consumer grade switch is daisy chained off one of the router ports. There is only one data line. The sales team have been given laptops which connect wirelessly when they are in the office and to any connection they can find when they are travelling. The company has an offsite hosted website for taking orders, keeping customer details and linking to an online payment service. It was written and is currently maintained by a local software developer.

The managing director has become aware of the possibility of cyber disasters after reading about ransomware attacks. He has contracted you to review his IT system and make recommendations.

You have visited the site for a review and discovered the following:

* You entered the industrial unit through a large door used for loading
* You went to the MD’s office and introduced yourself
* You noticed a server, printer and router on a side table
* You were given a user account to use with a password of guest
* In the general office you didn’t need to log in as a PC was on and unlocked
* The wireless network was unprotected
* The network switch was in the manufacturing section on a shelf
* You checked for open ports and found RDP was open to the internet
* You browsed to several dubious web sites
* On the way out you asked an employee if they knew about phishing: they didn’t.

## Task:

You now need to present

The most likely cyber threats that can involve a network the business needs to protect itself against.

The vulnerabilities you have found

How these vulnerabilities should be fixed

How the information should be protected

Required improvements to the network security

How the company can be fully cyber aware

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0-39 | 40-59 | 60-79 | 80-100 |
| **Executive summary and presentation** | Poor presentation. | Acceptable presentation. | Good presentation with clear narrative. | Good presentation with clear narrative, text and graphics. |
| **Threats and vulnerabilities** | Significant threats and vulnerabilities absent | Obvious threats and vulnerabilities covered | Threats and vulnerabilities covered with estimate of risk | Thorough explanation of threats and vulnerabilities, ranked in terms of risk |
| **Defence measures** | Some explanation of meeting requirements.  Minimal discussion of protocols | Reasonable explanation of meeting requirements.  Minimal discussion of protocols | Reasonable explanation of meeting requirements.  Reasonable discussion of protocols | Good explanation of meeting requirements.  Justified discussion of protocols |
| **Network and system improvements** | Network remains insecure | Basic security measures recommended | Comprehensive security measures recommended | Comprehensive security measures recommended with reasons |