Cyber Security Technician Final Portfolio and assessment

Scenario:

You are a cyber security consultant.

A small company with 45 employees makes, sells and installs garden sheds 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 and Site installation

Sales have been good during lockdown due to the demand for working at home and there is a backlog of orders. Consequently, 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 to load completed sheds
- 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
- You plugged in a USB stick so that you could copy information
- Apart from the finance and personnel folders you could copy and read anything on the file server
- You installed some software
- 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 write a formal report containing your recommendations. It must cover the following:

The most likely cyber threats that the business needs to protect itself against
The vulnerabilities you have found
How these vulnerabilities should be fixed
What policies should be put in place
How the information should be protected
Required improvements to the network security
What the responsibilities of management are
How the company can be fully cyber aware