Sheds and Things Initial Consultation

The below report consists of the findings I made during my visit to your premises and suggested on improvements to your security.

The areas of your business that are critical to it functioning are as follows:
The premises
As a manufacturer, all physical work occurs on site. In person customers visit the premises and meetings are held with them to discuss their needs. Incidents that occur in the here, whether these are crimes or natural disasters, will close the business resulting in a reduction of customers and manufacturing.

On Site IT Systems
These are parts of the IT infrastructure that are on-premises including printers, a wireless router, a file server, several PCs and a switch. This system is the easiest part of your IT infrastructure to protect as it is under your control.
Issues with the network can reduce productivity, if employees are unable to access their emails and worst case scenario put a halt to business if the company can't process/track new orders.

Off-site IT Systems
This includes portable devices (including laptops), the website and it's server. These have different kinds of risk compared to on-site systems due to the connections they have to the internet being essential to function. The website going down can result in a loss of revenue as online customers will not be able to make purchases, there is also the reputational impact of not being seen as secure. If a portable device is lost there is the potential for a data breach to occur which can result in a fine.

Observed Risks

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
Phishing attacks [High]	Unaware users are likely to fall for phishing scams [High]	Company Network [Critical]	Extended downtime from malware attack [Critical]	[High] Phishing scams and ransomware are increasly common	[High]	Educate employees in phishing techniques.
Malware – Malicious Websites	Dubious websites can be accessed from the network	Company Network [Critical]	Downtime from malware attack Data breach [Critical]	[High]	[High]	Install an application proxy at the edge of the network
Insecure passwords [High]	Weak password policy, permitting 5 letter passwords with no special character, numbers or upper case letters.	Desktops, server [Critical]	Compromise of system. Data exfiltration or risk of ransomware attack. [Critical]	[High] Opportunist password attacks are a regular threat.	[High]	Have a stronger password policy, requiring 14 characters, numbers, upper case letters and special characters.
Unauthorised access to the premises. [Moderate]	Unattended dock door [High]	Physical items. [Marginal]	Theft or damage of equipment. [Marginal]	[Low]	[Medium] Potential attack vector for a lot of other threats	-Close secondary entrances when not in use. -Limit customer access to sales area -Employees should approach anyone unfamiliar outside of the sales area.
Open ports increase attack surface.	RDP port open to the internet. [High]	Servers, desktops [Critical]	Compromise of system by attackers. [Critical]	[Medium] Websites like Shodan make it easy	[High] Compromise can result in hackers	If RDP is not necessary then disable it and ensure

[High]				for hackers to find open ports to attack.	controlling the system.	the port is closed. If essential, set up a terminal server or set up a company VPN and ensure RDP is only accessible from within the VPN.
Unauthorised access to confidential information. [High]	A permanently logged in account. [High]	Files on the network. [Moderate]	Critical data could be lost. Backup policy is unclear. [Critical]	[High]	[Medium]	Set the computer to log out after a moderate amount [5 minutes?] of inactivity[i]. Educate users in good security practices and encourage them to log off when leaving a device.
Installation of malicious software/malware. [High]	Users are able to install software, so anyone who gains access to a device can install a program. [High]	Enterprise network [Critcal]	The system can be infected by malware [Critical]	[High] Deliberate attacks are possible. Accidental issues due to poor user awareness more likely	[High] Malware attacks can have costly long term impacts.	Implement secure configuration settings and only allow administrators to install software.
Access to confidential information. [High]	A badly configured server allowing access to most files. [High]	Confidential data from the network [Critical]	Compromising the confidentiality, integrity and availability of data. [Critical]	[Moderate] Malicious attacks unlikely but accidents can occur	[Low] Requires access to physical device	Use Active Directory and Group Policy Settings for centralised control over users and devices, providing a

						more organised way of managing the network. Alternatively controlling file permissions using ACLs
Equipment can get accidentally/ deliberately damaged. [Medium]	Printer, router and server placed on side table. [Medium]	Printer, server, router [Critical]	Loss of internet connection, printer or file server access [Moderate]	[Low] It's unlikely anyone will be too careless	[Medium] Replacement hardware will be expensive.	Store server and router in a lockable cabinet[1] keep them out of harms way. Wall mount if space is an issue.
Theft of confidential files. [High]	Anyone is able to plug in a USB stick and copy files. [High]	Files on network [Moderate]	Theft of data. Potential fines for violating GDPR. [Critical]	[Low]	[Low] Requires extended physical access to devices.	Configure user accounts to deny access to USB ports by default.
Theft of client payment card information [High]	Customers paying through the website.	Confidential financial information [Critical]	Reputational damage [Critical]	[Low] Organisation has no interaction with customer financial information.	[Low] Risk transferred to third-party payment provider	
Unauthorised access to office areas [Moderate]	Unchallenged strangers in the office [High]	Information [Marginal]	Potential theft of personal information [Marginal]	[Low]	[Low]	Make anywhere outside of the sales area employees only and permit access to anyone else only when accompanied by a member of staff

1 https://www.cablemonkey.co.uk/371-data-server-cabinets

Malicious actors physically accessing company infrastructure [Low]	Router and server both accessible to anyone. It is possible to plug devices into them. [High]	Router, server [Critical]	Long term, persistent damage to business critical infratructure. [Critical]	[Low] Attacks require planning	[Low]	Storing the server and router in a lockable cabinet keep them out of harms way.
Disclosure of confidential information [High]	Lack of protocol for approaching the MD means that confidential conversations can be overheard [High]	Information [Marginal]	Potential theft of personal information [Marginal]	[Low]	[Low]	Staff will liaise between MD and customers. Assign a waiting area for customers.

The following is general advice to improve your security posture.

Management, Governance and Policies

Management Responsibilities

With issues such as cyber security it is important to lead from the top. Organisations with strong security culture are less vulnerable than others.
It is important to understand that a strong security culture does not equate to implementing the tightest controls all the time and that compromise between security and usability is essential. Users will find ways to bypass inconvenient security features to make life easier for themselves.

Management need to be aware and adhere to the law and different standards of data security.
- *The Computer Misuse Act*
Employees need to be aware of the computer misuse act. This can be done whilst onboarding, having them sign a document agreeing to comply with it.

- *Data Protection Act*[ii]
A law protecting personal data. It restricts the use of data and ensures it is kept for as little time as possible. Make sure that your company is following the legislation[iii].

- *GDPR*
Designed to protect the rights of EU/UK citizens worldwide. It prevents processing of personal data unless there is a legal reason to do so. In addition to this it specifies each organisation must have a Data Protection Officer, who is responsible for an organisation's data protection and privacy.

Incident response
There will be incidents in every organisation. Having an IR plan provides the whole organisation with a coordinated way to deal with incidents as they occur, clearly state who is involved and their responsibilities. A business continuity plan is a specific type of IR plan that is designed to keep the business running after it has been effected by a cyber attack.
It is important to reflect on incidents once they are over and learn from the mistakes that caused them.

Becoming Cyber Aware

Standards and frameworks have been created to help increase organisational awareness.

NIST Framework
Voluntary guidance based on existing standards designed to reduce cyber security risk and encourage cybersecurity management communications amongst stakeholders. The framework forms the foundation of a lot of organisation's security policies.

ISO 27001
This standards looks at information security leadership and supporting an information security management system. Through establishing an ISMS you will further identify the threats and opportunities around your business' assets.

Cyber Essentials
The NCSC is a good resource for educating employees.
Their Cyber Essentials scheme is designed to ensure participating organisations are protected against 80% of the most common attacks and the accompanying documentation is written in

layman's terms.
Another way to remain Cyber Aware is by using an online platform such as Immersive Labs that provides a gamified way of educating people and can be tailored to the need of your organisation.

Policy Implementation

Passwords
In addition to requiring use of upper case, symbols, numbers and 14 characters the following is good practice.
Require passwords to change every 60 days, have a minimum password age to stop them being changed immediately and enforce a password history to mitigate vulnerabilities caused by password reuse.

Backups[iv]
A strong backup policy can be the difference between minimal and extended amounts of downtime. Make sure to backup regularly. There are different kinds of backup, full, incremental (back up faster, recover slower) and differential (back up slow but recover fast). Good practice for backups includes having three copies, on two different forms of media, one of which is offsite.

Insider attacks
Insider threats are an issue. This is more likely to be a disgruntled employee than corporate espionage. Having a strong working culture can keep employees happy and on your side. Comprehensive onboarding & offboarding policies helps with this, making sure that former employees have their access rights removed.

Network Security

Asset Management
Keep track of what equipment and devices you own. One of the biggest security risks is devices running old versions of software or firmware. Having an inventory and a good patch/update management system is important.
Ensure all default configurations and passwords are changed.

Internet connectivity
Purchase VPN access for employees to use when working remotely. Public wifi is insecure and a VPN encrypts traffic, protecting it from eavesdroppers.

Install a stateful firewall downstream of the router to protect the network from internet traffic. These provide a greater level of protection that stateless firewalls, which operate on rules alone. Ensure the firewall is configured correctly, allowing minimal ports to have access to the internet. Insecure protocols such as Telnet should not be used.

Use enterprise equipment. Your consumer grade router lacks security features such as user authentication, PSKs are less secure than using a RADIUS server.

Strong Encryption
Use WPA3 on wifi networks and only allow TLS 1.3 connections when connecting to the internet. Earlier encryption standards such as WEP and SSL can be cracked.
Ensure website is
Provide each user with individual user accounts on the network to control their access.

User Account Configuration
Administrators should operate using the least privilege required for a task.
User accounts can be managed with group policies which can limit the access of users only to the groups you are assigned to.

Bring Your Own Device
Segment the BYOD part of the network. Implement Network Access Control [NAC] to ensure that devices meet minimum security standards.

Outsourcing
Ensure third parties are up to date with current secure working practices. Your web developer should be aware of OWASP, their list of common web vulnerabilities and mitigations.

i https://answers.microsoft.com/en-us/windows/forum/all/how-to-set-auto-logout-after-5-minutes-of-screen/16fe5231-3369-4857-954a-0abfe69ba98b
ii https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
iii https://www.gov.uk/data-protection-your-business
iv https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Backup-Policy-Template.pdf