Security Risk Assessment Report

Part 1: Chosen Hardening Tools and Methods

To help improve the organisation's network security and lower the risk of future breaches, I recommend putting the following three measures in place:

- **Multi-Factor Authentication (MFA)**
- **Firewall Maintenance and Port Filtering**
- **Strong Password Policies**

These steps focus on fixing the most serious gaps found during the review and are easy to apply consistently over time.

Part 2: Explanation of Recommendations

1. Multi-Factor Authentication (MFA)

What It Is:
MFA adds an extra layer of security by asking users to confirm their identity using two or more methods—such as a password plus a code sent to their phone, or a fingerprint scan.

What It Fixes:
Currently, the organisation doesn't use MFA at all. This means that if someone gets hold of a password, they could access the system without any extra checks.

Why It Matters:
Passwords alone are no longer enough. MFA helps protect accounts even if login details are stolen or guessed.

How It Helps Prevent Future Breaches:

- Blocks unauthorised access even if passwords are compromised
- Reduces the impact of phishing and brute-force attacks
- Makes it much harder for attackers to take control of key accounts

---

2. Firewall Maintenance and Port Filtering

What It Is:
This involves regularly reviewing and updating firewall settings and closing any unused or risky network ports. It's like setting clear rules about what's allowed in or out of the network.

What It Fixes:
Right now, the firewall has no rules in place. That leaves the network wide open to all kinds of traffic, including harmful connections.

Why It Matters:
A firewall is the first line of defence. Without proper settings, attackers can find easy ways in.

How It Helps Prevent Future Breaches:

- Keeps out suspicious or unwanted traffic
- Closes off access points that attackers often target
- Helps detect and block abnormal patterns like DDoS or malware traffic

---

3. Strong Password Policies

What It Is:
Good password policies make sure that staff create and use passwords that are secure, unique, and stored safely (e.g. with hashing and salting). These policies also make it clear that sharing passwords is not allowed.

What It Fixes:
Some staff are sharing passwords, and the admin account still uses its default password—this makes the network easy to break into.

Why It Matters:
Weak or shared passwords are one of the most common ways attackers gain access to systems.

How It Helps Prevent Future Breaches:

- Prevents easy password guessing and reuse
- Protects against brute-force and dictionary attacks

- Encourages a security-first mindset among employees

Conclusion

Setting up MFA, keeping firewalls properly maintained, and enforcing strong password rules are all essential steps in securing the network. These measures help fix key issues with access control and system protection.

By putting these methods into regular practice, the organisation will be much better prepared to stop future attacks, protect sensitive customer data, and build a stronger overall security posture.