Business Vulnerabilities Assessment – Small Business Scenario

1. Vulnerability Table:

- Weak password policy (High) — Implement strong password requirements.
- No MFA (High) — Enable multi-factor authentication.
- Outdated software (High) — Perform regular updates and patches.
- Shared accounts (High) — Assign unique accounts to all users.
- Open guest Wi-Fi (Medium) — Secure guest Wi-Fi and isolate networks.
- No firewall logging (Medium) — Enable and monitor firewall logs.
- Unlocked server room (High) — Restrict physical access.
- No data backup (High) — Implement daily automatic backups.
- No employee training (Medium) — Provide security awareness training.
- No incident response plan (Medium) — Establish IR plan with roles.

2. High-Risk Findings:

Weak passwords, missing MFA, outdated systems, no backups, open Wi-Fi, shared accounts, unlocked server room, and no logging.

3. Recommendations:

Technical: MFA, patching, backups, segmentation, firewall logging.

Administrative: IR plan, employee training, physical security, policies.

4. Summary:

This assessment identifies critical weaknesses in authentication, network security, physical security, backup policy, and user awareness. Mitigations are proposed to strengthen the organization’s security posture.