# Security risk assessment report

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers’ personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization’s network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization’s employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Firewall maintenance  Build a strong MFA  Password policies | |
|

| **Part 2: Explain your recommendations** |
| --- |
| As firewalls don’t have rules in this scenario the maintenance is required. To entail the checking and updating security configurations regularly to stay ahead of potential threats.  A strong MFA is required to prevent the future threats and risks . as it is not being used already and the password policies are also not maintained. MFA can be the great use to verify the authentications through the login credentials or using OTP.  The default password for databases need to change according time so this is one of the remediation that can be applied to prevent future malicious attack. |