# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Firewall rules  Stronger password policies (with MFA)  Encryption | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Updating the firewall by adding more rules to filter network traffic will filter out any unwanted packets that could cause harm to the network. The rules may need to be updated and or more added.  Enforcing a strong password policy will improve overall security of employees accounts and also help combat the use of default passwords as the employees will have to comply with this policy. Also with improving the password policy MFA can be used as this can also stop password sharing as the employees will need another way to authenticate either through SMS or google authenticator one-time-password. The password policy can be updated on occasions to comply with new standards.  Using encryption for the database is another technique that is used for if an attacker managed to get passed all the security controls and enter the database where all information in the database will be encrypted so the clients information cannot be read unless the hacker has an encryption key to decrypt the data making all the data useless to the attacker. |

Review the following scenario. Then complete the step-by-step instructions.

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.