# 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:

The organization’s employees' share passwords.

The admin password for the database is set to the default.

The firewalls do not have rules in place to filter traffic coming in and out of the network.

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** |
| --- |
| 1. Strong Password Policies  2. Firewall Configuration  3. Implementing Multifactor authentication  Multi-Factor Authentication (MFA) requires users to authenticate their identity through multiple methods before accessing an application. These methods can include fingerprint scans, ID cards, PIN numbers, and passwords.  Password policies can be strengthened by setting rules for password length, acceptable characters, and including disclaimers to discourage password sharing. These policies can also define consequences for unsuccessful login attempts, such as locking the user out of the network after five failed attempts.  Regular firewall maintenance involves routinely checking and updating security configurations to stay ahead of potential threats. |
|

| **Part 2: Explain your recommendations** |
| --- |
| Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. MFA significantly reduces the likelihood of unauthorized access through brute force or related attacks, as it requires multiple forms of authentication. Additionally, MFA discourages password sharing, as the recipient would also need to possess the additional authentication method, making password sharing less effective and less likely.  Creating and enforcing a comprehensive password policy within the company can further protect against unauthorized access. Policies such as suspending accounts after a certain number of failed login attempts can prevent successful brute force attacks. Additionally, increasing password complexity, requiring more frequent updates, and disallowing password reuse all contribute to stalling malicious actors and protecting the network.  Regular firewall maintenance is also critical for network security. Network administrators should ensure that firewall rules are current and reflect the latest standards for allowed and denied traffic. Suspicious traffic sources should be added to a denied list. Firewall rules should be promptly updated following any security events, particularly those involving suspicious network traffic, to protect against various DoS and DDoS attacks.  These combined measures—MFA, robust password policies, and regular firewall maintenance—form a multi-layered defense strategy, significantly enhancing network security and reducing the risk of unauthorized access. |