# Security risk assessment report

## Scenario

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.

| **Part 1: Select up to three hardening tools and methods to implement** |
| --- |
| 1. **Multifactor authentication (MFA)**<br>2. **Firewall Rules**<br>3. **Password policies** |

**Part 2: Explain your recommendations**

**1. Implementation of Multifactor Authentication (MFA):**
A strong defense system known as multifactor authentication (MFA) requires users to submit many pieces of identification before being granted access. Typically, this entails either something they are (biometric data) or something they have (a mobile device or hardware token). Even if a user gives an attacker their password via phishing or credential stuffing, they will still require the second factor to access the system. As a result, credentials that have been stolen work much less effectively. The organization considerably raises the bar for unwanted access attempts by deploying MFA for all accounts, especially those with access to important systems and data.

**2. Network segmentation and firewall rules:**
Firewalls protect an organization's internal network from outside attacks. Organizations can determine what kinds of communications are allowed or prohibited by establishing a thorough ruleset. The firewall helps stop malicious activity and unauthorized access attempts by filtering both incoming and outgoing traffic. By separating the network into distinct segments, network segmentation goes one step further. Critical systems, such databases that house client data, are set up in separate segments with limited access. As a result, attackers who compromise one region of the network are unable to rapidly move laterally and get access to other important parts. It's a preventative measure to lessen the potential effects of a breach.

**3. Password Management and Policy:**
Implementing a strong password policy requires establishing standards for password complexity, such as a minimum length, a combination of uppercase and lowercase letters, digits, and special characters. Passwords are made tough to guess or crack thanks to this policy. However, it can be difficult to rely only on users to generate secure passwords and remember them. A password management tool can help with this. The need for users to remember complex passwords is reduced by these technologies, which generate and store them for each account. Password managers also assist in preventing the reuse of passwords across many accounts, which lowers the possibility of attackers getting access to multiple systems in the case that one password is compromised. Employees are regularly educated about security risks and the value of using strong passwords.