# Security risk assessment report

**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** | |
| --- | --- |
| Multi-factor authentication to authenticate employees.  Stronger password policies need to be implemented. No sharing of passwords is allowed.  Addition of an intrusion protection system (IPS), and intrusion detection system(IDS)  Firewall configuration and maintenance to prevent data exfiltration | |
|

| **Part 2: Explain your recommendations** |
| --- |
| I recommend multifactor authentication as it provides an extra layer of security beyond only a password and it is another method to authenticate the identity of employees. Shared passwords are a threat to overall network security as it could fall into the hands of a malicious actor which is why MFA needs to be implemented to authenticate users that gain access to the network  Stronger password policies need to be implemented: 8 letters, 1 number, and a special character minimum. Password resets need to be enforced within a timeframe of 2 months. A no-sharing of password policy needs to be implemented  The addition of an Intrusion Protection System (IPS) will be beneficial as it will monitor systems for signs of intrusive activity and take steps to stop the intrusion  The Intrusion Detection System will be beneficial to achieving a better security posture because it will monitor systems for signs of intrusion and provides a real-time alert to possible intrusions.  Firewall maintenance should happen regularly. Network administrators should  ensure that firewall rules are in place that reflect the most up-to-date standards for allowed and denied traffic. Traffic from suspicious sources should be placed on a denied traffic list. Firewall rules should be updated whenever a security event occurs, especially an event that allows suspicious network traffic into the network. |