# Security risk assessment report

*Google cyber security Assessment:*

*Context: 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** | |
| --- | --- |
| If we analyse the situation we can clearly state that the organization is lacking in the structure of their defense, **Employees are sharing their password which is not permissible and will result in lots of issues such as accessing unauthorized accounts and potentially bank accounts (we don’t know how specific the password sharing is)**.  **The admin password for the database is set to default which also means most of the people can access the database.**  **Firewall deemed not be structured as well, and no rules are built upon it..**  **MFA is also not used which causes issues..**  **Therefore the following methods should be implemented:**   1. Enabling Password policies 2. MFA 3. Maintain FIrewall | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Password policies are essential as they prevent easy guessing of passwords. These policies may include one-time passwords or biometric authentication like fingerprints. In this instance, employees were sharing passwords, necessitating the implementation of strict password policies and education for all employees.   A password policy is a set of rules designed to enhance security by enforcing strong, unique passwords and proper password management practices. For example, requiring passwords to be at least 12 characters long, containing a mix of letters, numbers, and special characters., by doing so they will be setting up and following the NIST standard  To address the current issue:   1. Reset all employee passwords. 2. Ensure all employees use a password manager. 3. Educate employees on the importance of not sharing passwords. 4. Change the database admin password from its default to a secure, secretive one.   2. The company should adhere to Apply MFA Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained. Like for example setting up a one time password.  3. The company should also maintain and take care of setting up firewall rules This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. |