# Security risk assessment report

Benjamin Taylor – Google Cybersecurity

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** |
|---|
| • Password Policies<br>• Firewall Maintenance<br>• Multi Factor Authentication |

## Part 2: Explain your recommendations

- Enforcing strong and unique passwords as well as prohibiting the use of old/default passwords will help prevent brute force and credential-based attacks.
- Regularly reviewing and updating firewall rules will make sure that only authorized traffic flows in/out of the network, reducing risk of external threats (DoS, intrusion, etc.)
- Requiring users to provide multiple verification forms before accessing systems is crucial because it can prevent unauthorized logins, even if credentials are compromised.