# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| In terms of Network Hardening to prevent the next data breach.   1. **Port Filtering** - We need to add this firewall function in order to block or allow certain port numbers to limit unwanted communication for the Social Media Organization - We need to have the most Up-To-Date Network/Wifi Protocols in Data Restriction Zones to avoid data breaches. 2. **Network Access Privilege** - Need to assign specific rights and abilities to specific authorized users distinct from administration privileges. 3. **Encryption** - Transform Readable Data into an encodable format to prevent unauthorized use of data and preserve the Confidentiality and Integrity of user data. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. **The organization’s employees' share passwords.**    1. We do not recommend that employees do not share passwords at all as this can cause an issue in the organization. This violates the confidentiality and integrity of a password being used by an unauthorized user which can be detrimental to the organization itself.   Policies used in the organization can prevent attackers from easily guessing passwords manually or by using a script to attempt thousands of stolen passwords from Brute Force Attacks  *\*Network Access Privilege, Password Policies/Guidelines*   1. **The admin password for the database is set to the default.**    1. After the default password is configured on an organization’s network it is recommended at the Industry Standard Level that a long complex password would be implemented for the user as well as additional authorization such as 2FA or MFA. Default passwords can be easily guessed by an attacker.   \**Network Access Privileges, Multi-Factor Authentication, Encryption using the latest standards, Password Policies.*   1. **The firewalls do not have rules in place to filter traffic coming in and out of the network.**    1. FIrewalls need to be able to allow or block unwanted communication especially for the network’s port numbers for Internet and Email. While packets are incoming and outgoing on the network we believe more network security applications from *Next Generation Firewalls*, as well as a combination of *Intrusion Detection System* and *Intrusion Prevention System* would be very ideal (\*NGFW / IDS / IPS) To have these embedded on an Organization’s Network Topology would be ideal in order to enhance network security.   Another tool that would be ideal to monitor the network is the Security Information Event Management Tool (SIEM) in order to monitor the network activity and system and make necessary decisions that need to be implemented.  *\*Firewall Maintenance, Port Filtering.*   1. **Multi Factor authentication (MFA) is not used.**     1. In relation to recommendation #2 for additional Hardening Tasks for security especially for user access admin password, more additional authorization to authorize a user would be very ideal to add another layer of security.    2. This preserves the integrity of the user authorization access and will help keep the user secure on the network. This can help further protect from brute force attacks and other similar security events   *\*Multi Factor Authentication Implementation, Encryption - Latest Standards* |