Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
There were 4 Major Vulnerabilities that were discovered during inspection. They were: 1) Shared passwords among employees 2) Admin password was set to default 3) Firewalls do not have rules in place to filter network traffic 4) MFA was not in use The best way to mitigate these risks is to implement: 1) Enforce Password Policies 2) Enable Port Filtering and/or Firewall Maintenance 3) Enable MFA (Multi Factor Authentication)

Part 2: Explain your recommendations
As discussed before, we have seen that there were 4 major vulnerabilities which led to the data breach. First, we recommend enforcing password policies, this is to reduce the likelihood of an attacker using a brute force attack to guess employee or default passwords - which would give them the opportunity to infiltrate our database. Second, enabling port filtering will strengthen our firewall with the ability to block or allow certain port numbers to enter, limiting unwanted communication. In addition to that we would like to recommend regularly maintenance firewalls, this entails checking and updating security configurations. This is to reduce the likelihood of allowing abnormal network traffic into the network and preventing another major data breach Lastly, We have found that MFA was not used which is a crucial point in strengthening our network. This makes sure that each employee or admin is able to verify that they themselves are trying to access certain data.