Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1) **Password Policies:** Implement password policies in compliance with NIST standards to ensure passwords remain secure and difficult to harvest. 2) **Firewall Maintenance:** Since the current firewalls do not have rules in place to filter traffic coming in and out of the network, implement regularly scheduled firewall maintenance in order to establish updated security configurations. 3) **Multifactor Authentication (MFA):** Current security measures at the organization do not call for the use of MFA. In order to enhance security, establish password MFA systems so only authorized actors can gain access to sensitive information.

Part 2: Explain your recommendations
Password policies ensure that all employee/organization passwords remain secure according to standards set up by organizations such as NIST. Secure and safe passwords decrease the chances of malicious actors guessing, solving, or harvesting passwords that can access sensitive and crucial company and personal data using brute force methods. Implementing firewall maintenance ensures that possible intrusions get filtered out by the system, securing the overall network from harmful attacks. It can also help to stop major cybersecurity threats such as DoS attacks. Finally, MFA methods would allow for even more secure systems by requiring a second step of verification, such as a text message received to your phone, in order to check if an authorized user is accessing the data.