Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The three hardening tools that need to be implemented as a response to the data breach is as follows : 1. It is noticed that the organization's employees' shared passwords and admin password is set to default. The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. ● Security Hardening Task : Password Policy 1. Making use of strong and unique passwords for all employees and regularly changing passwords 2. Not making use of a default password for admin, and access being given only to the designated workers 2. It is also noticed that firewalls do not have rules in place to filter traffic coming in and out of the network. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. ● Security Hardening Task : Firewall Maintenance 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. 3. Lack of MFA (Multi-Factor Authentication) exposes a vulnerability, which may result in a data breach in the future. A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. ● Security Hardening Task : Multi Factor authentication (MFA)

Part 2: Explain your recommendations
Password Policies Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).
Multi Factor authentication (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.
Firewall maintenance Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.