Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three network security hardening tools the organisation can used to address vulnerabilities found: 1. Firewall maintenance 2. Multi-Factor authentication (MFA) 3. Password policies Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. MFA is 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. For password policies, the organization can follow the National Institute of Standards and Technology's (NIST) latest recommendations for password policies where it focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. They can also enforce no sharing of password and admin's password to follow rules such as password length, a list of acceptable characters. They can also limit login attempts such that after 5 unsuccessful attempts to login, accounts will be locked out.

Part 2: Explain your recommendations
Firewall maintenance should happen regularly to ensure they are providing adequate protection against threats. Firewall rules should be updated and reviewed at least once a year or whenever a security event occurs to ensure they are up to date and restrictive enough. This can ensure any potential breaches in the future. Scheduled firewall audits should also occur to assess firewall's configuration and effectiveness, which can help identify any potential gaps before they are exploited.

Enforcing Multi-Factor Authentication (MFA) significantly reduces data breaches by adding an extra layer of security beyond just a password. Even if an attacker compromises a user's credentials through phishing or other means, they would still need the second authentication factor, such as a time-sensitive code, biometrics, or a physical device, to access the account. This additional requirement makes unauthorized access much more difficult, thereby protecting sensitive data from potential breaches.

Enforcing strong password policies reduces data breaches by ensuring passwords are complex, regularly updated, and unique, limiting the risk of unauthorized access. In cases of password sharing, mandatory changes and unique requirements for each user minimize the effectiveness of shared credentials. Replacing default admin passwords with strong, custom ones prevents attackers from exploiting widely known default credentials, significantly enhancing security within the organization. Passwords must also be changed once every few months to ensure no security breaches.