Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Based on the recent data breach at the organization in which sensitive customer data was exposed, including names and addresses and upon investigation, four critical vulnerabilities were identified: password sharing among employees, the use of a default admin password for the database, the absence of firewall rules, and the lack of multifactor authentication. If these issues remain unaddressed, the organization risks future cyberattacks and potential regulatory violations. To mitigate these risks, three essential hardening techniques should be implemented: Enforcing strong password policies Configuring firewalls with strict rules Implementing multifactor authentication

Part 2: Explain your recommendations
Enforcing strong password policies is key to preventing unauthorized access to sensitive systems. Employees should be required to create complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Also, password sharing should be firmly prohibited, and password managers should be used to store credentials securely. Implementing regular password changes and educating employees about the dangers of weak passwords will further enhance security. Additionally, configuring firewalls with strict rules is essential for monitoring and controlling network traffic. Firewalls should be set up to allow only necessary traffic while blocking unauthorized connections. Regular updates to

firewall rules should be conducted to ensure they adapt to emerging threats. Additionally, integrating intrusion detection and prevention systems will provide an added layer of security by identifying and mitigating malicious activities before they cause harm.

Implementing multifactor authentication adds an extra layer of security by requiring users to verify their identity using multiple authentication methods, such as a password and a one-time code sent to their mobile device. Even if an attacker obtains login credentials, they will be unable to gain access without the second authentication factor. MFA should be enforced across all critical systems, especially for administrative and privileged accounts, to minimize the risk of unauthorized access.

By implementing these network hardening techniques, the organization can significantly reduce its exposure to cyber threats and prevent future breaches. Strengthening password security, enforcing strict firewall configurations, and adopting MFA will create a more resilient security posture and protect both company and customer data from potential attacks.