# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Tool/Method 1: Password Policy Enforcement with Strong, Unique Passwords**  * **Description:** Implement mandatory password policies requiring strong, unique passwords, regular password changes, and strict prohibition of password sharing. * **Reason for Effectiveness:** Significantly reduces the risk of unauthorized access by preventing attackers from exploiting weak, reused, or shared passwords, protecting against brute-force attacks and leaked credentials.  **Tool/Method 2: Firewall Configuration with Traffic Filtering and Restrictive Rules**  * **Description:** Deploy and configure network firewalls with specific rules to block unauthorized traffic, control ports and protocols, and limit connections to trusted sources only. * **Reason for Effectiveness:** Creates a robust security barrier that prevents external and internal unauthorized access, protects against exposed services exploitation, lateral movement, malware, and data exfiltration.  **Tool/Method 3: Implementation of Multi-Factor Authentication (MFA)**  * **Description:** Enforce MFA for all critical systems, including corporate email, servers, databases, and administrative platforms. * **Reason for Effectiveness:** Even if credentials are compromised, MFA prevents attackers from gaining access without the second authentication factor, protecting against phishing, credential theft, and social engineering attacks. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The recommended hardening methods directly address the vulnerabilities that led to the data breach. Here’s why they are essential and how they improve the organization’s security:   1. **Password Policy Enforcement**  Implementing a strong password policy is critical because shared or weak passwords are one of the most common causes of security breaches. By requiring complex, unique passwords and regular updates, the risk of unauthorized access through credential stuffing, brute-force attacks, or insider threats is greatly reduced. This protects both employee accounts and administrative systems. 2. **Firewall Configuration with Traffic Filtering**  Firewalls are the first line of defense against external threats. Without proper filtering rules, malicious traffic can enter or leave the network unnoticed. By setting restrictive rules, only legitimate and necessary traffic is allowed. This prevents attackers from scanning, exploiting open ports, or moving laterally within the network, drastically reducing the attack surface. 3. **Multi-Factor Authentication (MFA)**  MFA is one of the most effective security controls. Passwords alone are not enough because they can be leaked, guessed, or stolen. MFA adds an additional layer of verification, such as a code sent to a mobile device or biometric authentication. This means that even if a password is compromised, an attacker cannot access the account without the second authentication factor. MFA greatly enhances protection for sensitive systems like databases, email, and administrative tools. |