# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| I think the biggest vulnerability that the company should address is our Access and identity issues.  We can address this issue by implementing these network hardening tools   * Multi factor authentication * Stricter password policies * Firewall mantinence | |
|

| **Part 2: Explain your recommendations** |
| --- |
| I believe that multi factor authentication is important because we dont want unauthorized or unwanted users to have access to information that they are not entitled to.  Stricter password policies would help because. It was brought to my attention that some employees share passwords. So if we set up the correct parameters (only use strong passwords, limited attempts before account lockout) and inform employees about how what they are doing is putting the company at risk then that could be a good deterrent for malicious actors.  Firewall maintenance is another tool that we could benefit from. I say this because our firewall wasnt configured correctly and could have saved us from the previous breach . But the firewall didnt have any rules set up so its almost the same as not having one. So if we configure it correctly and do routine updates to the rules based on current trends and threats it can increase security posture. |