# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Given the current situation, the nature of the breach, and current known vulnerabilities I would implement these three things:   * New and updated Password Policies * MFA (SMS, email, application) * Routine firewall maintenance | |
|

| **Part 2: Explain your recommendations** |
| --- |
| The password policy will include:   * employees/customers will need to create a new password upon their first attempt to log in after implementation. * All current admin accounts will also have their passwords reset and changed where possible to reflect the new policy below. * New password complexity requirements:   + Passwords now must be a minimum eight characters long and a max of twenty characters   + cannot contain the employees/customers name (first, middle, or last)   + must include at least one special character (! @ # $ % ^ & \* ( ) \_ + - = { } [ ] | \ : ; " ' < > , . ? / ~ `)   + A minimum of one lower case   + A minimum of one upper case   + A minimum of one number   + A new written policy added to the company internal technology agreement stating password sharing is not allowed and will result in possible disciplinary action for the employees involved.   Given the abrupt nature and newnest of this policy for the employees specifically, the policy will only lock their account after ten wrong tries within fifteen minutes and then they will be required to contact the help desk for a reset. One month after implementation that will be reduced to five wrong tries within fifteen minutes to better ensure workflow.  For customers after ten wrong tries within ten minutes their account will be locked and they will be sent an email stating as such and to provide them a way to reset their password.  Enabling MFA for both employee and customers:   * employees will be required to use MFA delivered by the google authenticator application on their work phones. Upon entering their password correctly it will prompt them to then supply the code given by google authenticator. * Customers will be given the option to use MFA if they so choose with their options being sms, email, or authenticator app (any that take the supplied code/QR code to link). When signing up for a new account users will be supplied a screen asking for them to set it up with the option to opt out. Current users will be given the same screen on their next new login after MFA goes live.   Firewall maintenance will now be in effect as an ongoing responsibility of the company’s SOC team. Firewall rules and configurations are now being audited internally every month to ensure new rules and configurations are being added as often as is necessary to ensure it remains updated with the newest and best practices and also updated against the newest threats.  Both the new password policy and enabling MFA is a combined approach to cover the current vulnerabilities and to upgrade the company's security posture. The new complexity requirement will help prevent brute force attacks, while the forced password reset will ensure all passwords for both employees and customers meet the new requirements. Stopping password sharing between employees is not possible. The new internal policy with us now requiring MFA should help reduce it to the bare minimum.  The added firewall maintenance will just overall increase the whole security posture of the company as a whole unit and will further increase our Defense in-depth strategy. |