Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Due to the data breach, security analysts recommend implementing the following solutions: ● Password policy ● Network access permissions ● MultiFactor authentication (MFA)

Part 2: Explain your recommendations
Password policy - Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). **Network access permissions** - Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc. Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once, or revisited depending on the likelihood of social engineering or brute force attacks. **MultiFactor authentication (MFA)** - 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.

Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then maintained.