Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Three hardeinging tools and methods to inmlement into the system to decrease the amount of data creaches would be adding a multifactor authentication MFA, update password policies, and update firewalls. I would also even suggest updating network access privileges.

Part 2: Explain your recommendations

It is important to implement multifactor authentication to implement the users to verify their identity in two or more ways to access a system or network. This can include an extra password, pin number, badge, one-time password (cell phone/email), fingerprints and even more. Suggesting this will decrease the amount of attempts due to the addition layer of security as the malicious hacker must then go through another phase of defense.

Updating password policicies such as focusing on specific methods that will make a brute force attack much more difficult and complex and by doing so will require many more possibilities making it difficult to break through.

Lastly, because the data breach also had no rules to filer regularly it was difficult to stay ahead of any potential threats. Therefore by checking and updating security configurations regularly to stay ahead of potential threats it will become increasingly harder to penetrate ones account.

Lastly, my suggestion of updating network access privileges limit the access involving, permitting, limiting, and or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses and etc. This means that sharing of passwords will also decrease as well as reducing the risk of unathroized suers and outside traffic from accessing the internal network. Very beneficial to brute force attacks as well.