Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
It's recommended to implement, Password Policies, Network Access Privileges and Firewall Maintenance.

Part 2: Explain your recommendations
Due to the nature of the attack, possibly a breach due to weak credentials, it is important to implement strong Password Policies that prevent users to share the same password or previous passwords. It's important to have a strong policy that prevents user from setting weak (and common) passwords, as well as prevent the use of default credentials on databases and users logins. The second recommendation is to implement, Network Access Privileges. This prevents unauthorized clients to access restricted information by limiting/ blocking access from unknown devices. This implementations limits access to data to certain clients with a specific IP/MAC address. Because this could be implemented once and maintained when needed, it will be one of the most impact-to-effort ratios for the business. The third implantation is to have a strong Firewall Policy and Maintenance. This prevents unfiltered data to reach the internal (restricted) servers and unfiltered data to exit the network. Combining Password Policy with Network Access Privileges and a Good Firewall Maintenance could prevent future breaches. With these implementations the system will be fortified against weak credential use, a privileged based access to network assets, decreasing the likelihood of social engineering or brute force attacks and with a strong Firewall to only allow filtered results to access the internet and filtered results to arrive at the internal network.

Note: There could be other implementations used to prevent this type of breach from happening again. I have chosen these Security Hardening Tasks due to their effectiveness. Although altering Baseline Configurations, Multi-Factor Authentication, Port Filtering and actively Pen Testing the network would be

good measure to implement and encouraged, fortifying the network has a greater impact than basic configuration and actively testing for new exploits. Having good, uncrackable passwords with the additional user based access will protect the network from hops between devices. Additionally filtering the content allowed to exit or to enter the restricted network — again with user based authentication — will improve the security of the system and prevent unexpected data leakage.