Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The first tool to implement would be MFA. This would include emailing a one time password, or a phone notification, any secondary check of identity commonly through another trusted device. The second method recommended is using NIST password policies. This means following the standards set by NIST for every employee username and password in the organization. This would make every password significantly harder to breach given a specified complexity. It would also completely disrupt password sharing. The third method is regular firewall maintenance. There should be a set schedule for this and it includes the tasks of filtering traffic based on potential attacks that are visible in anomalous network traffic, such as a Ddos attack. It also includes updating the security settings of the firewall to stay protected against new vulnerabilities.

Part 2: Explain your recommendations
Without multi factor authentication the chance of a successful attack is much bigger. This is set up once and prevents brute force attacks and requires two forms of identity confirmation meaning a potential threat actor could be prevented from access even if they have evaded one form of identification. Given that employees share passwords and the database password is the default, implementing these policies will completely eliminate many potential threats, especially internal ones. Firewall maintenance was not occurring and is a recognized threat to the organization's security posture. Updating these rules and security settings to stay protected by recognizing suspicious network traffic will prevent many attacks.