Security Risk Assessment Report

Part 1: List a few hardening tools and methods to implement
1. Multi factor authentication (MFA) 2. Network access privileges 3. Password policies

Part 2: Explain your recommendations
Multifactor authentication (MFA), network access privileges, and password policies are three essential security measures that can help prevent data breaches. Let's explore how each of these measures contributes to data breach prevention: 1. Multifactor Authentication (MFA): MFA adds an extra layer of security to the authentication process by requiring users to provide multiple forms of verification to access their accounts or systems. Typically, this involves combining something the user knows (e.g., a password) with something they possess (e.g., a unique code sent to their smartphone) or something inherent to them (e.g., biometric data like fingerprint or facial recognition). By implementing MFA, even if a malicious actor obtains someone's password, they would still need access to the additional verification factors to gain entry. This significantly reduces the risk of unauthorized access, as it becomes much more challenging for attackers to bypass multiple layers of security. 2. Network Access Privileges: Network access privileges refer to the level of permissions and restrictions granted to users or devices within a network. By carefully managing and assigning access privileges, organizations can control who can access sensitive data and what actions they can perform. Implementing the principle of least privilege ensures that users only have

access to the resources necessary to perform their job functions. This practice minimizes the potential damage that could occur if an account is compromised or misused. By limiting access to sensitive data and critical systems, the impact of a data breach can be contained, as attackers would face obstacles when attempting to escalate their privileges within the network.

3. Password Policies:
Password policies establish guidelines for creating and managing passwords within an organization. They typically define requirements such as password complexity, length, expiration, and restrictions on reuse. Implementing strong password policies encourages users to create robust and unique passwords, which are harder for attackers to guess or crack.

By enforcing password policies, organizations can reduce the risk of successful brute-force attacks or credential guessing. Additionally, regular password changes help mitigate the impact of compromised passwords, as even if a password is leaked or stolen, it becomes invalid after a certain period.

Overall, these three measures work together to enhance data breach prevention. MFA ensures that unauthorized users cannot easily gain access, network access privileges limit the scope of potential damage, and password policies create barriers against password-related attacks. Implementing these measures as part of a comprehensive security strategy significantly strengthens an organization's defenses and reduces the likelihood of successful data breaches.