# Solution Guide: Considering Security and Business Objectives

## Business Plans

1. The director of engineering suggested giving all developers access to all data.

    - **Pros**: Makes development easier.
    - **Cons**: Allows *any* developer to access *any* user data, including sensitive PII that has nothing to do with their jobs.

    **Recommendation**: The business should **reject** on grounds of privacy.

2. The director of IT suggested exposing administration servers to the public internet.

    - **Pros:** Administrators can work from any computer.
    - **Cons:** The servers would be publicly accessible, which is unacceptable for a private network.

    **Recommendation**: The organization should **reject** this request. A VPN would be a better solution to this problem.

3. An SOC analyst recommended merging all of the company's mail servers into a single server, in order to cut costs and improve SOC efficiency.

    - **Pros:** It would ultimately cost less and reduce the number of servers that attackers could potentially compromise, the number of machines that could expose vulnerabilities, and the number of machines that SOC has to monitor.
    - **Cons**: If the company has so many emails that it *needs* to maintain multiple servers, this suggestion won't be possible.

      **Recommendation**: If the company doesn't have so many emails that multiple servers are necessary, hosting all of the data on a single machine is a good idea.

## Security Recommendations

1. The director of security suggested implementing a private corporate VPN.

    - As an added layer of security, a VPN would prevent unwanted outsiders from entering the corporate network and keep sensitive data confidential. Business practices will change significantly, requiring onboarding and training of all employees.

    - While the initial onboarding and training will require upfront work, the added security benefits down the road are worth it. The organization should accept this request.

2. The director of engineering suggested requiring all developers to use SSH keys instead of passwords to communicate with internal SSH servers. They plan to block password access in two weeks.

    - Cryptographic SSH keys are more secure than vulnerable passwords that can be cracked. The organization should accept this request.

3. The security team suggested hardening the merged mail server via encryption or placing the mail server behind a firewall and only allowing access from the corporate VPN.

    - In general, encryption is not a good idea. It requires a lot of power to encrypt and decrypt data, and email doesn't usually contain confidential data.

    However, selectively encrypting emails that do contain encrypted data is a good idea.

    - Only allowing access to the mail servers from the corporate VPN also seems a bit of an extreme measure.

      Again, email usually does not contain confidential information, so access does not need to be so strictly controlled.

      However, this approach might make sense in environments with lots of confidential information, such as government agencies, law firms, or medical records companies.