2.2.3 Defense Planning Facts

Layered security, or defense in depth security, is a security approach that combines multiple security controls and defenses to create a cumulative effect.

Layered Security has seven layers, which are explained in the table below:

Security Layer	Description
Policies, Procedures, and Awareness	Includes user education, manageable network plans, and employee onboarding and off-boarding procedures.
Physical	Includes fences, door locks, mantraps, turnstiles, device locks, server cages, cameras, motion detectors, and environmental controls.
Perimeter	Includes firewalls using ACLs and securing the wireless network.
Network	Includes the installation and configuration of switches and routers, implementation of VLANs, penetration testing, and virtualization use.
Host	Includes each individual workstation, laptop, and mobile device. The Host layer includes log management, OS hardening, patch management and implementation, auditing, malware, and password attacks.
Application	Includes authentication and authorization, user management, group policies, and web application security.
Data	Includes storing data properly, destroying data, classifying data, cryptography, and data transmission security.

It is important to know that each layer does not require its own security appliance or software. Layered security is not about specific mechanisms, but the method of protecting a network by employing various techniques at one time.

Employees are the single greatest threat to network security. Therefore, user education is very important. Look for ways to take the following actions:

- Train employees so they know that employees are the primary targets in most attacks.
- Ensure employees understand that phishing attacks are one of the most common attacks directed at employees.
- Ensure that employees can identify email, instant messaging, download, and website attacks.
- Enforce effective password policies, including a policy that prohibits writing down passwords.
- Train employees to identify both internal and external threats.
- Ensure that employees are aware of the company's security policies.

A countermeasure is a way to mitigate a potential risk. Countermeasures reduce the risk of a threat agent being able to exploit a vulnerability. An appropriate countermeasure:

- Provides a security solution to an identified problem.
- Is not dependent on secrecy.
- Is testable and verifiable.
- Provides uniform or consistent protection for all assets and users.
- Is independent of other safeguards.
- Requires minimal human intervention.
- Is tamper-proof.
- Has overrides and fail-safe defaults.