1.2.3 Defense Planning Facts

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

This lesson covers the following topics:

- The seven layers of security
- User education
- Countermeasures

The Seven Layers of Security

Layered security has seven layers. The following table describes each layer.

Security Layer	Includes:
Policies, procedures, and awareness	User education; manageable network plans; and employee onboarding and off-boarding procedures.
Physical	Fences, door locks, mantraps, turnstiles, device locks, server cages, cameras, motion detectors, and environmental controls.
Perimeter	Firewalls using ACLs and securing the wireless network.
Network	The installation and configuration of switches and routers; implementation of VLANs; penetration testing; and virtualization use.
Host	Log management, OS hardening, patch implementation, patch management, auditing, anti-malware, and password attack prevention on each workstation, laptop, and mobile device.
Application	Authentication and authorization, user management, group policies, and web application security.
Data	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.

User Education

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

- Make employees aware that they are the primary targets in most attacks.
- Ensure employees understand that phishing attacks are one of the most common attacks directed at employees.

- Train employees to 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.

Countermeasures

A countermeasure is a way to mitigate a potential risk. Countermeasures reduce the risk of a threat agent exploiting 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.