



Item of system equipment, such as hardware, firmware, software, or documentation

Facility that houses system operations and equipment

Service provided by a system

Data contained in an information system

System capability, such as processing power or communication bandwidth

Action, device, or technique that reduces a threat, vulnerability, or attack

Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result

Assault on system security that derives from an intelligent threat

Intelligent act that is deliberate attempt to evade security services, and violate the security policy of a system

Set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Flaw or weakness in a system's device, implementation, or operation and management that could be exploited to violate the system's security policy

Entity that attacks or threatens a system

Possible danger that might exploit a vulnerability

Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

minimizing the harm it can cause

eliminating or preventing it

discovering and reporting it so the corrective action can be taken