W06 Vocabulary: Data Protection

Administrative Countermeasures

Term	Definition
policy	A brief statement of goals, ends, desires, or purposes. (It answers the question, “What should happen?”)
procedure	A collection of detailed plans and prescriptions for how a policy is pursued and implemented. (It answers the question, “How should it happen?”)
acceptable use policy	A policy that defines the actions users may perform while accessing systems and network equipment.
email policy	A policy that defines appropriate use of email communications.
control	A tool to regulate or guide security efforts; can be preventive, detective, corrective, etc.
least privilege	Providing only the minimum authorization necessary to perform a duty or task.
physical security	Systems and technologies that are not computer information systems, but can be used to help protect computer information systems.

Responses to Risk

risk	A situation that involves exposure to danger.
accept	Acknowledge risk without addressing it.
avoid	Abandon a potentially dangerous activity.
mitigate	Make a risk less serious.
transfer	Make another party assume responsibility for a risk.

Device Countermeasures

screen lock	An access control mechanism that prevents use of a device until an unlocking action is successfully performed.
backup	A copy of information system's data, to preserve it in case of loss or destruction of the system or its information.
system hardening	Disabling unused services, changing default accounts/passwords, and updating or patching a system.
AV (antivirus)	Software to detect and prevent execution of worms and viruses.

Network Countermeasures

air gap	A physical boundary between information systems, in which devices in one system are not and have never been networked to devices or data in the other system.
blacklist	A collection of forbidden actions or items.
whitelists	A collection of permitted or allowed actions or items.
default deny policy	A stance of forbidding everything except what a whitelist specifically allows.
firewall	A device or software to control the kinds of transmissions that are denied (blacklisted) or permitted (whitelisted) on a network connection.
single point of failure	A component of a system, which, if it stops functioning properly, adversely affects the entire system.
redundancy	Duplicating a resource, to eliminate single points of failure and ensure availability.

Cryptography Related Jargon

cryptography	The science of transforming data in order to use, store, or transmit it securely.
algorithm	A mathematical procedure or recipe that may be used to transform data.
key	A secret collection of numbers or keystrokes used by a cryptographic algorithm.
encryption	Using an algorithm with keys to transform data, making it unintelligible to everyone except intended recipients.
decryption	Using an algorithm with keys to recover encrypted data.
plaintext	Understandable data, before it is encrypted or after it is decrypted.
ciphertext	Encrypted data.
cleartext	Plaintext that is transmitted clearly instead of transformed into ciphertext before transmission.
cryptanalysis	Attempts to recover plaintext from ciphertext with limited or no knowledge of the algorithm or keys.
cipher	An encryption algorithm that substitutes characters for other characters.
brute force attack	Exhaustively test every possible input (usually passwords) until one is found that produces a desired result.
dictionary attack	Attempt to guess a password by trying words from a dictionary or from a similar list of candidates.