# Security+ chapter 1

A user copies files from her desktop to a USB Flash Drive & puts the device into her pocket. Which security goals is most at risk? Confidentiality

Smart phones with cameras and Internet capabilities pose a risk to which security goal? Confidentiality

By definition, which security concept ensures that only authorized parties can access data? Confidentiality

You computer system is a participant in an asymmetric cryptography system. You've crafted a message to be sent to another user. Before transmission, you hash the message, then encrypt the hash using your private key. You then attach this encrypted hash to your message as a digital signature before sending it to the other user.

In this example, what protection does the hasing activity ptovide?

Integrity

Which of the following is an example of an internal threat?

A user accidentally deletes the new product designs.
A delivery man is able to walk into a controlled area & steal a laptop.
A water pipe in the server room breaks.
A server backdoor allows an attacker on the Internet to gain access to the intranet site.

A user accidentally deletes the new product designs.

What is the greatest threat to the confidentiality of data in most secure organizations?

Hacker intrusion

Malware

USB Devices

Operator error

USB Devices

Which of the following is the correct definition of a threat?

Any potential danger to the confidentiality, integrity, or availability of information or systems.

Absence or weakness of a safeguard that could be exploited.

The likelihood of an attack taking advantage of a vulnerability.

Instance of being exposed to losses from an attacker

Any potential danger to the confidentiality, integrity, or availability of information systems.

Which of the following is an example of a vulnerability?

Mis-configured server

Virus infection

Denial of service attack

Unauthorized access to confidential resources

Mis-configured server

Which of the following is not a valid concept to associate with integrity?

Control access to resources to prevent unwanted access.

Ensure your systems record the real information when collecting data

Prevent the unauthorized change of data

Protect your environment so it maintains the highest source of truth.

Control access to resources to prevent unwanted access

When a cryptographic system is used to protect the confidentiality of data, what is actually protected? Unauthorized users are prevented from view or accessing the resource.

By definition, which security concept uses the ability to prove that a sender sent an encrypted message? Non-repudiation

The company network is protected by a firewall, an IDS, and tight access controls. All of the files on this protected network are copied to tape every 24 hours.

The backup solution imposed on this network is designed to provide protection for what security service?

Availability

ONSECURITY+ CHAPTER 1 SPECIFICALLY FOR YOUFOR ONLY$13.

90/PAGEOrder NowTags:

- Cryptography