**Cyber Security**

**Fundamentals**

**Information, Computer & Network Security**

Information Security refers to the protection of available information or information resources

from unauthorized access, attack, theft, or data damage.

Responsible individuals and organizations must secure their confidential information.

Computer security is the protection of computer systems and information from harm, theft,

and unauthorized use.

Network security is the protection of the underlying networking infrastructure from

unauthorized access, misuse, or theft.

**Vulnerabilities**

At the most basic level, a vulnerability is any condition that leaves an

information system open to harm.

Vulnerabilities can come in a wide variety of forms, including:

• Improperly configured or installed hardware or software.

• Delays in applying and testing software and firmware patches.

• Untested software and firmware patches.

• Bugs in software or operating systems.

• The misuse of software or communication protocols.

• Poorly designed networks.

• Poor physical security.

• Insecure passwords.

• Design flaws in software or operating systems.

• Unchecked user input

Dr. Risala Tasin Khan

#

**Threats**

In the realm of computer security, a threat is any event or action that

could potentially cause damage to an asset.

Threats are often in violation of a security requirement, policy, or

procedure.

Regardless of whether a violation is intentional or unintentional,

malicious or not, it is considered a threat.

Potential threats to computer and network security include:

• Unintentional or unauthorized access or changes to data.

• The interruption of services.

• The interruption of access to assets.

• Damage to hardware.

• Unauthorized access or damage to facilities.

Authentication

Authentication is the method of validating a particular

entity's or individual's identity and unique credentials.

Authentication concentrates on identifying if a particular

individual has the right credentials to enter a system or

secure site.

Authentication credentials should be kept secret to keep

unauthorized individuals from gaining access to

confidential information.

#

**Authorization**

In security terms, authorization is the process of determining what rights and

privileges a particular entity has.

Authorization is equivalent to a security guard checking the guest list at an

exclusive gathering, or checking for your ticket when you go to the movies.

After a user has been identified and authenticated, a system can then determine

what rights and privileges that user should have to various resource:

Access Control

Accounting and Auditing

Principle of Least Privilege

Privilege Management