# Introduction to Information Security

## Lecture 01

Kashif Ali

BSCS 5th FGHI

Subject: Information Security



# What is Information Security (InfoSec)?

- Information security, often referred to as InfoSec, refers to the processes and tools
  designed and deployed to protect sensitive
  business information from modification, disruption, destruction, and inspection.
- This includes policy settings that prevent unauthorized people from accessing business or personal information.
- InfoSec is a growing and evolving field that covers a wide range of fields, from network and infrastructure security to testing and auditing.

# Information Security vs Cybersecurity


- Information security differs from cybersecurity in both scope and purpose.
- The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security.
- Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security.
- It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.

- Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them.
- Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.

# Application Security


- Application security is a broad topic that covers software vulnerabilities in web and mobile applications and application programming interfaces (APIs).
- These vulnerabilities may be found in authentication or authorization of users, integrity of code and configurations, and mature policies and procedures.
- Application vulnerabilities can create entry points for significant InfoSec breaches.
- Application security is an important part of perimeter defense for InfoSec.

# Cloud Security

- Cloud security focuses on building and hosting
  secure applications in cloud environments and
  securely consuming third-party cloud applications.
- “Cloud” simply means that the application is running in a shared environment.
- Businesses must make sure that there is adequate isolation between different processes in shared environments.

# Cryptography

- Encrypting data in transit and data at rest helps
  ensure data confidentiality and integrity.
- Digital signatures are commonly used in cryptography to validate the authenticity of data.
- Cryptography and encryption has become increasingly important.
- A good example of cryptography use is the Advanced Encryption Standard (AES).
- The AES is a symmetric key algorithm used to protect classified government information.

kashif.nth@aup.edu.pk

# Infrastructure Security

- Infrastructure security deals with the protection of internal and extranet networks,
  labs, data centers, servers, desktops, and mobile devices.


kashif.nth@aup.edu.pk

# Incident Response


- Incident response is the function that monitors
  for and investigates potentially malicious behavior.
- In preparation for breaches, IT staff should have an incident response plan for containing
  the threat and restoring the network.
- In addition, the plan should create a system to preserve evidence for forensic analysis and potential prosecution.
- This data can help prevent further breaches and help staff discover the attacker.

# Vulnerability Management

- Vulnerability management is the process of scanning an environment for weak points (such as unpatched software) and prioritizing remediation based on risk.
- In many networks, businesses are constantly adding applications, users, infrastructure, and so on.
- For this reason, it is important to constantly scan the network for potential vulnerabilities.
- Finding a vulnerability in advance can save your businesses the catastrophic costs of a breach.


DISCUSSION
QUESTIONS