WILEY

SYBEX
A Wiley Brand

# CompTIA IT Fundamentals Study Guide (FC0-U61)

## Chapter 9:

## Security Concepts and Threats

# Chapter 9: Security Concepts and Threats

- Explain the value of data and information
  - Data and information as assets
  - Importance of investing in security
  - Relationship of data to creating information
  - Intellectual property
    - Trademarks
    - Copyright
    - Patents
  - Digital products
  - Data-driven business decisions
    - Data capture and collection
    - Data correlation
    - Meaningful reporting
- Summarize confidentiality, integrity, and availability concerns
  - Confidentiality concerns
    - Snooping
    - Eavesdropping
    - Wiretapping
    - Social engineering
    - Dumpster diving
  - Integrity concerns
    - Man-in-the-middle
    - Replay attack
    - Impersonation
    - Unauthorized information alteration
  - Availability concerns
    - Denial of service
    - Power outage
    - Hardware failure
    - Destruction
    - Service outage

# Chapter 9: Security Concepts and Threats (con't.)

- Compare and contrast authentication, authorization, accounting, and non-repudiation concepts
  - Authentication
    - Single factor
    - Multifactor
    - Examples of factors
      - Password
      - PIN
      - One-time password
      - Software token
      - Hardware token
      - Biometrics
      - Specific location
      - Security questions
    - Single sign-on
  - Authorization
    - Permissions
    - Least privilege model
    - Role-based user access
      - User account types
    - Rule-based user access
    - Mandatory access controls
    - Discretionary access controls
  - Accounting
    - Logs
    - Tracking
    - Web browser history
  - Non-repudiation
    - Video
    - Biometrics
    - Signature
    - Receipt

# Understanding Hackers and Motives

- Stealing passwords or personal information
- Gaining remote access to a server or an operating system
- Logging in locally and stealing data
- Changing a website's content
- Gaining access to the contents of a database (perhaps one that contains passwords or credit card information)
- Surreptitiously analyzing network traffic
- Installing software designed to cause harm or steal data
- Creating a condition in which a computer or network no longer works well
- Modifying existing software so that it no longer performs as it should or so that it secretly does harmful things in addition to its usual activity

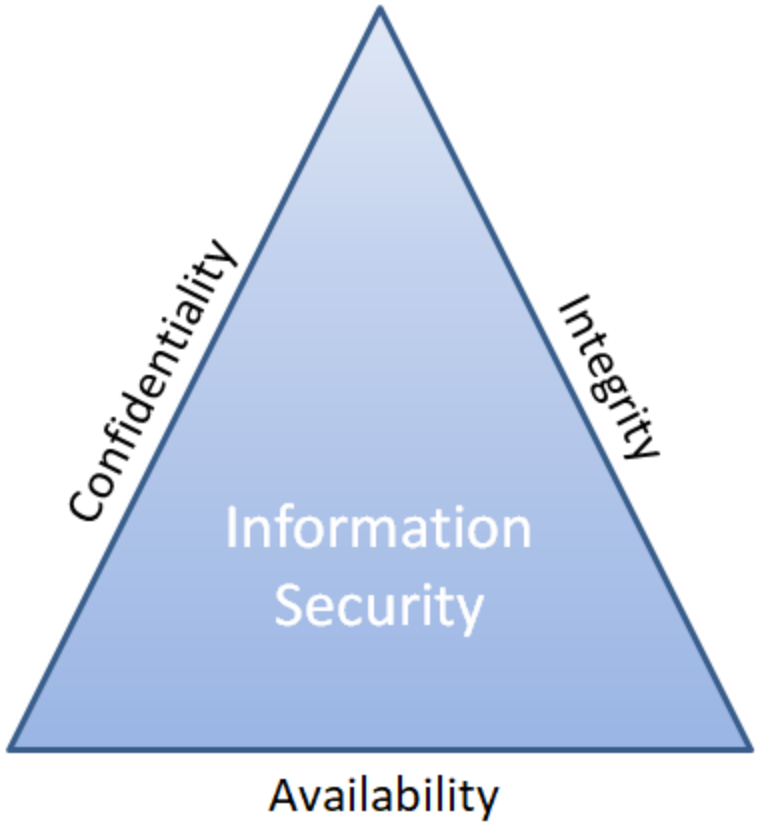
# The Value of Data

- Data as a driver of business decisions
- Intellectual property
  - Trademarks
  - Copyright
  - Patents
- Digital products

SYBEX
A Wiley Brand

# Understanding Security Threats

- CIA triad




WILEY

# Confidentiality Concerns

- Snooping
- Eavesdropping
- Wiretapping
- Social Engineering
  - Phishing
  - Shoulder surfing
- Dumpster diving

# Integrity Concerns

- Man-in-the-middle attack
- Replay attack
- Impersonation
- Unauthorized information alteration

# Availability Concerns

- Denying service
- Hardware concerns
  - Hardware damage
  - Hardware theft

# Software-Based Security Threats

- OS and Application Exploits
- Viruses
- Worms
- Trojan horses
- Adware
- Spyware
- Ransomware
- Rootkits
- Backdoors
- Spam
- Password cracking

# Understanding Access Control

- Triple A:
  - Authentication
  - Authorization
  - Accounting
  - (and non-repudiation)

# Authentication

- Validates identity
- Types of authentication
  - Single-factor
  - Multifactor
  - One-time password
  - Smart card or security token
  - Location-specific
  - Biometrics
- Single sign-on (SSO)

# Authorization

- Determines what users can do

- Mandatory access control
- Discretionary access control
- Role-based access control
- Rule-based access control

# Accounting

- Records who does what

- OS and application logs
- Web browser history