Security Planning

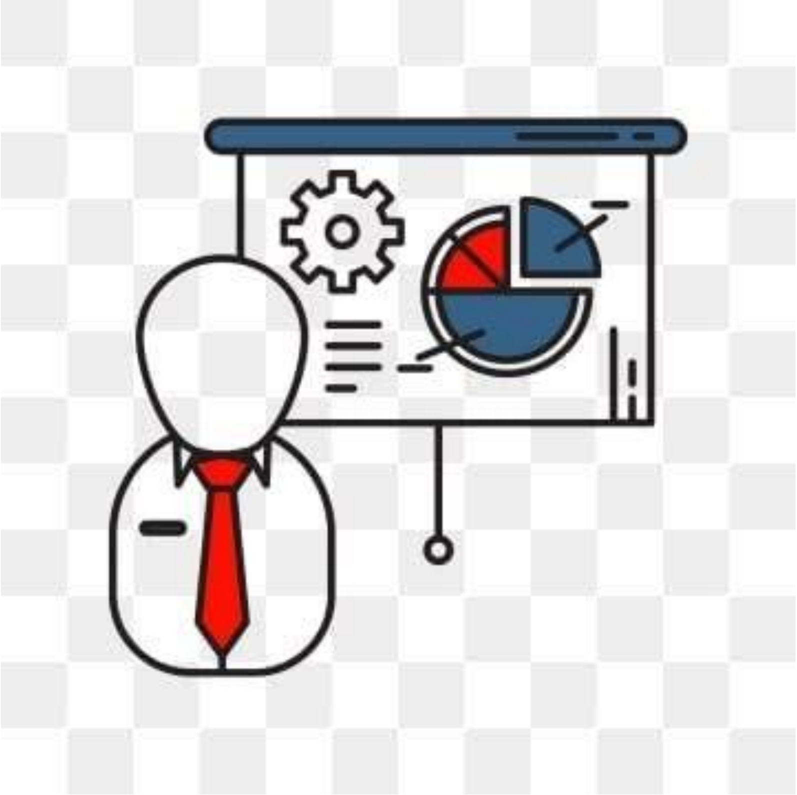
Principles of information security

SASKATCHEWAN POLYTECHNIC

Tomorrow in the making

Outline

- Definition of Information Security
- Information Security vs Cybersecurity
- Principles of Information Security
- Authentication, Authorization, Accountability (AAA)
- Impact of Organizational Attributes on Information Security
- Computer Security Terminology



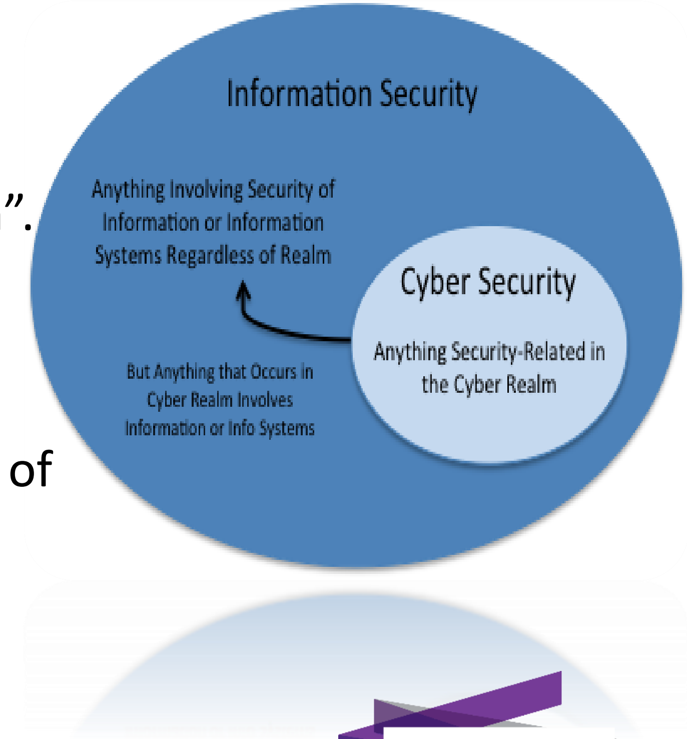
Information Security

- The National Institute of Standards and Technology (NIST) of US defines the term Information security as follows:
  - “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.”
  - The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Sources: NIST SP 800-59 under Information Security from 44 U.S.C., Sec. 3542 (b)(1), [44 USC 3502 (8)]

Principles of Information Security

- Information Security vs Cybersecurity
- Based on the ISO/IEC 27032:2012, Cybersecurity is defined as the “preservation of the confidentiality, integrity, and availability of information in Cyberspace”.
- Information Security, on the other hand, is defined as the: “preservation of the confidentiality, integrity, and availability of information”.
- In the digital age, information security is critical for protecting sensitive data, maintaining trust, and the main objective is to ensure the continuity of business processes with the least damage and limit the negative impacts of incidents.


Information Security
Anything Involving Security of Information or Information Systems Regardless of Realm
Cyber Security
Anything Security-Related in the Cyber Realm
But Anything that Occurs in Cyber Realm Involves Information or Info Systems

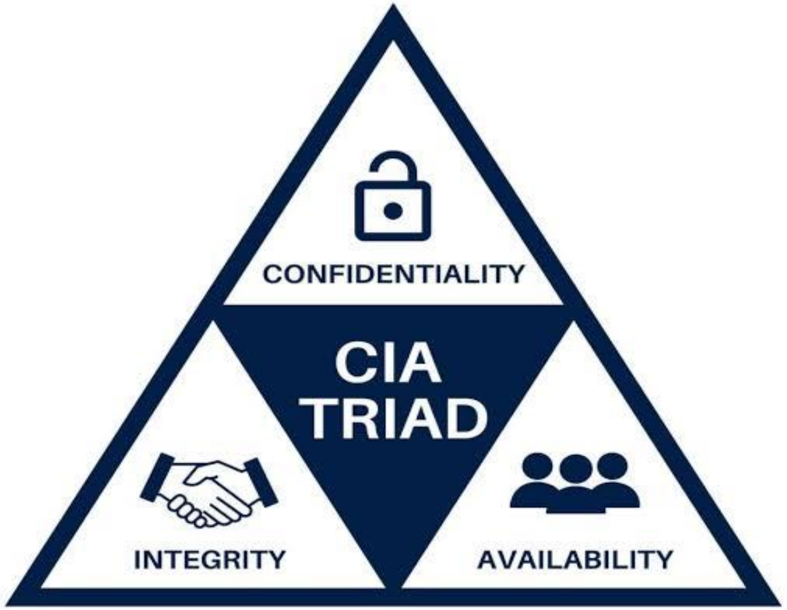
Information Security fully includes Cybersecurity as one of its components.

Principles of Information Security

- The NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) lists confidentiality, integrity, and availability as the three security objectives for information
  - FIPS stands for Federal Information Processing Standards (FIPS)

Principles of Information Security

- CIA Triad
  - Confidentiality – Integrity – Availability
  - Your processes should always be guided by these three principles
    - Are you keeping your data confidential?
    - Does your approach help guarantee the integrity of data?
    - Does your approach still make the data readily available to authorized users?



Principles of Information Security

- Confidientiaity
  - Involves protecting information from unauthorized disclosure.

    Measures include encryption and access controls. Measures include encryption and access controls.

    Examples: Personal data, trade secrets.
- Integrity
  - Focuses on maintaining the accuracy and reliability of information. Safeguards against unauthorized modifications.

    Examples: Data integrity checks, checksums.
- Availability
  - Ensures that information and systems are accessible when needed.
    - Involves redundancy, backup systems, and disaster recovery.

      Examples: Redundant servers, backup data centers.

Principles of Information Security

- Confidentiality
  - Attackers cannot read intercepted messages
  - Confidentiality can be provided by encryption
  - Refers to the characteristic of information whereby only those with sufficient privileges may access certain information
  - Measures used to protect confidentiality
    - Access Controls
    - Information classification
    - Secure document storage
    - Application of general security policies
    - Education of information custodians and end users

Principles of Information Security

- Confidentiality
  - Covers two related concepts:
    - Data confidentiality
    - Privacy

Principles of Information Security

- Integrity
  - Assurance that data is not altered
  - Provided by hashing data
  - Refers to the quality or state of being whole, complete, and uncorrupted
  - Information integrity is always threatened if exposed to corruption, damage, destruction, or other disruption of its authentic state
  - Corruption can occur while information is being compiled, stored, or transmitted

Principles of Information Security

- Integrity
  - Covers two related concepts
    - Data Integrity
    - System Integrity

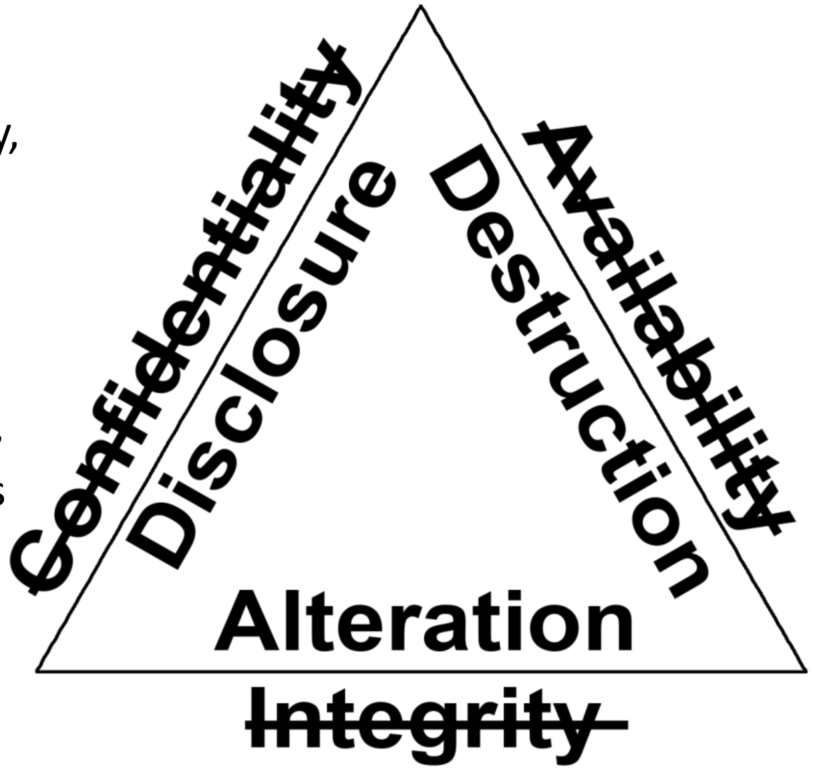
Principles of Information Security

- Availability
  - Network available to all appropriate users
  - Provided by authentication

  - Refers to the characteristic of information that enables user access to information in a required format, without interference or obstruction
    - A user in this definition may be either a person or another computer system
  - Availability does not imply that the information is accessible to any user, but rather implies availability to authorized users

Principles of Information Security

- DAD
  - While the CIA triad—serves as the cornerstone of information security, it's equally important to explore the inverse of these principles. We must be aware of potential threats that pose the opposite challenges.
  - Let's delve into the counterparts of these key principles—**Disclosure**, **Alteration** and **Destruction**—examining the risks and vulnerabilities that can compromise the security of our information.

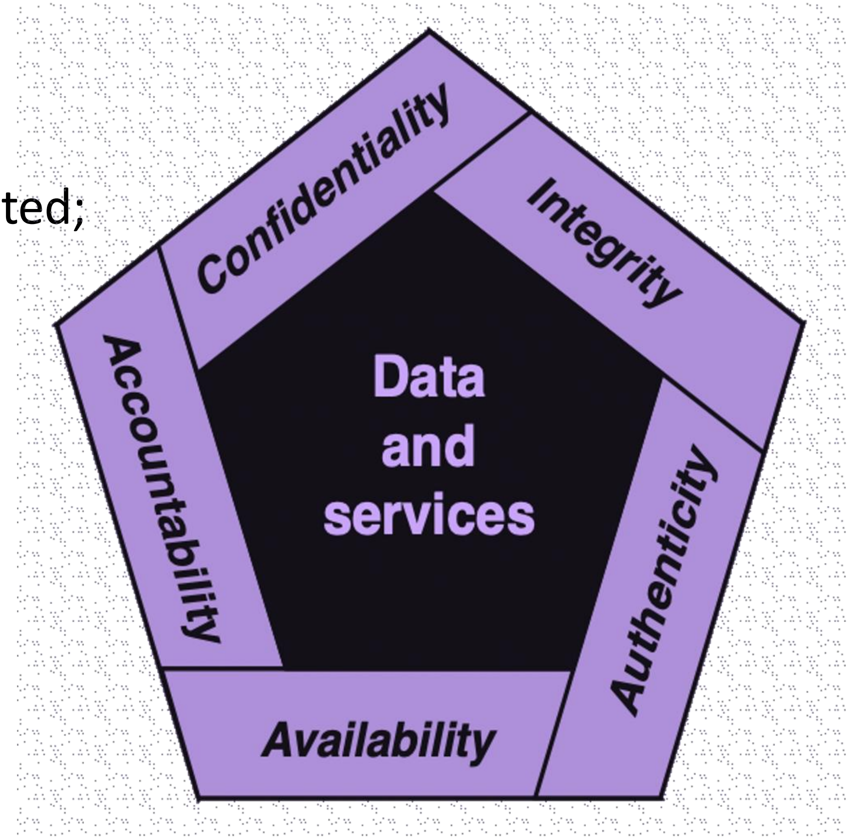


Principles of Information Security

- DAD
  - Disclosure The exposure or revelation of information to individuals, entities, or systems that are not authorized to access it. This unauthorized access can lead to a breach of confidentiality, as sensitive or confidential data becomes accessible to those who shouldn't have that privilege
  - Alteration - Unauthorized modification or change of data. It is a concept closely tied to the integrity aspect of the CIA triad. Data integrity ensures that information remains accurate, consistent, and unaltered during its lifecycle. When data alteration occurs, it means that the information has been changed in a way that was not intended or authorized.
  - Destruction - The intentional or unintentional loss, deletion, or removal of data, making it permanently or temporarily unavailable

Principles of Information Security

- Additional concepts
  - Authenticity
    - being genuine and being able to be verified and trusted;
  - Accountability
    - being able to be traced
  - Non-repudiation
    - Prevents denial of authentic actions.
    - Involves digital signatures and audit trails.
    - Examples: Digital signatures in contracts



- FIPS 199

Authentication Authorization Accountability (AAA)

- Authentication (aka verification)
  - Who are you?
  - Occurs when a control verifies the identity of a user
    - User may be a person or a computer
  - Aka Verification

- Authorization
  - What can you do?
  - Occurs when a control verifies the actions that an user can do
    - E.g. access, update, or delete content
  - Authorization occurs after authentication.

Authentication Authorization Accountability (AAA)

- Accountability
  - Can the activity be traced back to a unique/specific user?
  - Exists when a control can verify that certain operations or activities have been performed by a specific user.

Cyber Attack Scenario

Impact of Organizational Attributes on Information Security

- ## Organizational Culture
  - Influences attitudes towards information security.
  - Building a security-aware culture is crucial. Examples: Employee mindset, cultural norms.
- ## Leadership and Management
  - Strong leadership commitment is essential.
  - Management decisions influence resource allocation.

    Examples: CEO commitment, budget allocation.
- ## Organizational Structure
  - Affects the assignment and management of security responsibilities.
  - Clear reporting lines enhance information security. Examples: Security roles, reporting structure.
- ## Risk Management
  - Balancing risk and business objectives.
  - Identifying and addressing vulnerabilities. Examples: Risk assessments, mitigation strategies.

Impact of Organizational Attributes on Information Security

- Technology Infrastructure
  - The type of technology impacts security measures.
  - Regular updates and patches are essential. Examples: Firewalls, antivirus software.
- Regulatory Compliance
  - Organizations must comply with industry and regional regulations.
  - Compliance impacts security controls. Examples: GDPR, PCIDSS, HIPAA.
- Employee Behavior
  - Human factors play a crucial role in information security.
  - Training and awareness programs are critical. Examples: Phishing incidents, insider threats.

Computer Security Terminology

- Adversary
  - Individual, group, organization, or government that conducts or has the intent to conduct detrimentaL activities. Examples: Security roles, reporting structure.
- Attack
  - Actions by threat actors (individual or group) who try to gain unauthorized access , steal data or cause damage to the computer system and/or other resources.
- Counter measure
  - A device of techniques that has as its objective that impairment of the operationa effectiveness of undesireable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or sensitive information systems
- Risk
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurence

Computer Security Terminology

- Security Policy
  - A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- System Resource (Asset)
  - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
- Threat
  - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other or the Nation through an information destruction, disciosure, modication of information and/or denial of service:
- Vulnerability
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Computer Security Terminology

- Computer Security Terminology, from RFC 2828, Internet Security Glossary, May 2000
  - https://www.ietf.org/standards/rfcs/.
  - https://tools.ietf.org/html/rfc2828

References

- Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). Computer security: principles and practice (pp. 978-0). Upper Saddle River, NJ, USA: Pearson Education.
- https://www.researchgate.net/publication/366716821_Cybersecurity_vs_Information_Security
- https://www.youtube.com/watch?v=GX_XsdNv1PY

SASKATCHEWAN
POLYTECHNIC

Tomorrow
in the making

saskpolytech