**Information Security**

* **Goal**: Prevent unauthorized disclosure of information.
* **Focus**: Information flow; confidentiality is primary.

**Bell-LaPadula (BLP) Model**

* **Purpose**: Ensures confidentiality by preventing unauthorized disclosure.
* **Key Concepts**:
  + **Security Levels**: Top Secret, Secret, Confidential, Unclassified.
  + **Rules**:
    - **No Read Up (ss-property)**: A subject can read objects at or below their security level.
    - **No Write Down (\*-property)**: A subject can only write to objects at or above their security level.
  + **Discretionary Security (ds-property)**: Access must adhere to specified permissions.
  + **Limitations**:
    - Balancing confidentiality and integrity.
    - Classification changes over time.
    - Complexity in shared resources.
* **Applications**: Role-based access control (e.g., teacher-student roles).

**Biba Integrity Model**

* **Focus**: Data integrity across security levels.
* **Rules**:
  + **Simple Integrity**: Modify only if subject's integrity level ≥ object's.
  + **Integrity Confinement**: Read only if subject's level ≤ object's.
  + **Invocation Property**: Subjects of lower levels cannot invoke higher-level subjects.

**Clark-Wilson Integrity Model**

* **Focus**: Practical enforcement of data integrity.
* **Key Features**:
  + **Well-formed Transactions**: Users manipulate data in constrained ways.
  + **Separation of Duty**: Creation and execution of transactions are segregated.
  + **Data Types**:
    - **Constrained Data Items (CDIs)**: Sensitive data like financial records.
    - **Unconstrained Data Items (UDIs)**: General data.
  + **Procedures**:
    - **Integrity Verification Procedures (IVPs)**: Ensure data remains consistent.
    - **Transformation Procedures (TPs)**: Manage valid state transitions.
* **Rules**:
  + Certification (e.g., TPs must maintain valid states).
  + Enforcement (e.g., user authentication during transactions).

**Chinese Wall Model**

* **Purpose**: Addresses confidentiality and conflict of interest.
* **Key Concepts**:
  + **Datasets (DS)**: Information grouped by corporation.
  + **Conflict of Interest Classes (CI)**: Prevent access to competing corporate data.
  + **Access Control**:
    - Based on access history.
    - Once a dataset is accessed, conflicting datasets are restricted.

**Comparison**

* **Bell-LaPadula**: Focuses on confidentiality, history-less, security levels fixed.
* **Chinese Wall**: Focuses on conflict of interest, access control evolves with access history.

**Introduction**

* Organizations must understand their legal and ethical responsibilities.
* InfoSec professionals should:
  + Stay updated with laws and regulations.
  + Monitor emerging issues to minimize risks and liabilities.

**Law and Ethics**

* **Laws**: Mandate/prohibit behaviors and are enforced by the state.
* **Ethics**: Define socially acceptable behaviors but lack enforcement.
* **Cultural Mores**: Group-specific moral attitudes or customs.
* **Liability**: Legal obligation extending beyond criminal/contract law, including restitution for harm caused.

**Policy vs. Law**

* Policies are internal rules specifying acceptable employee behavior.
* Enforcement criteria: dissemination, review, comprehension, compliance, uniform enforcement.
* Unlike laws, ignorance of a policy can be a valid defense.

**Types of Law**

1. Constitutional
2. Statutory (civil, criminal)
3. Regulatory/Administrative
4. Common (case law)
5. Private/Public laws

**Cyber Laws in Pakistan**

* **Electronic Transaction Ordinance (2002)**: Legal recognition of electronic documents.
* **Electronic Crimes Bill (2007)**: Defined cyber offenses like forgery, stalking, data damage.
* **Prevention of Electronic Crimes Act (PECA 2016)**:
  + Covers all Pakistanis and crimes affecting Pakistani data/persons.
  + Major offenses:
    - Unauthorized access: 5 years, Rs. 5 million.
    - Unauthorized interference: 7 years, Rs. 10 million.
    - Cyberstalking: 3 years, Rs. 1 million.
    - Cyber terrorism: 14 years, Rs. 50 million.
  + Investigated by FIA's Cybercrime Wing.

**International Cyber Laws**

* Few enforceable global laws exist due to cultural and political differences.
* **WTO's TRIPS Agreement**: Protects intellectual property rights globally.

**Digital Millennium Copyright Act (DMCA)**

* U.S. law to reduce copyright/trademark infringement.
* Prohibits:
  + Circumvention of security protections.
  + Manufacturing/trafficking circumvention tools.
  + Altering copyright-embedded information.

**Ethics in Information Security**

* Many professions prescribe ethical behavior; InfoSec lacks binding codes.
* **Ten Commandments of Computer Ethics** (e.g., don’t harm, snoop, or steal via computers).
* Cultural differences affect perceptions of ethical behavior.

**Deterring Unethical Behavior**

* Causes: ignorance, accident, intent.
* Effective deterrence requires:
  + Fear of penalty.
  + High probability of being caught.
  + Certain enforcement of penalties.

**Professional Organizations**

* **ACM**: Focuses on confidentiality, intellectual property.
* **(ISC)²**: Develops security certifications (e.g., CISSP).
* **SANS Institute**: Offers GIAC certifications.
* **ISACA**: Focuses on auditing, control, and InfoSec standards.
* **ISSA**: Facilitates InfoSec education and networking.

**Summary**

* Laws and ethics govern behavior; organizations must ensure due care and diligence.
* Ethical training and adherence to codes of conduct are vital for InfoSec professionals.

………………………………………………………………………………………………………………………………………………………………….

**Intrusion**

* **Definition**: Attempt to break into or misuse a system by external or internal users.
* **Classes of Intruders**:
  + **Masquerader**: Unauthorized outsider exploiting legitimate accounts.
  + **Misfeasor**: Insider misusing authorized access.
  + **Clandestine User**: Gains supervisory control, evading access controls.

**Intrusion Detection System (IDS)**

* **Definition**: Monitors and analyzes system events to detect unauthorized access in real time.
* **Components**:
  + **Sensors**: Collect data (network packets, logs, system calls).
  + **Analyzers**: Determine if an intrusion occurred.
  + **User Interface**: Displays system outputs and controls.

**IDS Principles**

1. Quick detection minimizes damage and accelerates recovery.
2. Acts as a deterrent to intrusion attempts.
3. Collects data to strengthen security measures.

**Types of IDS Detection**

1. **Anomaly-Based Detection**:
   * Learns legitimate behavior and flags deviations.
   * Strength: Detects novel attacks.
   * Weakness: High false positive rates.
2. **Signature-Based Detection**:
   * Uses predefined attack patterns to identify threats.
   * Strength: Accurate for known attacks.
   * Weakness: Cannot detect novel attacks.
3. **Hybrid Detection**:
   * Combines strengths of anomaly and signature-based methods.
   * Includes specification-based intrusion detection.

**Effectiveness of IDS**

* Must detect a high percentage of intrusions while maintaining low false alarms.
* Challenges include balancing accuracy and efficiency.

**Host-Based vs. Network-Based IDS**

* **Host-Based**:
  + Monitors individual systems and application logs.
  + Strengths: Attack verification, real-time detection.
  + Weaknesses: Selective logging risks missing attacks.
* **Network-Based**:
  + Analyzes network traffic in real time.
  + Strengths: Cost-efficient, real-time response.
  + Weaknesses: Limited in detecting encrypted attacks.

**Intrusion Prevention System (IPS)**

* **Definition**: Detects and prevents malicious activities, including blocking or dropping malicious traffic.
* **Detection Types**:
  + **Signature-Based**: Matches known attack patterns.
  + **Anomaly-Based**: Detects deviations from normal behavior.
  + **Policy-Based**: Uses custom-defined security rules.

**Honeypots and Deception Technology**

* **Honeypots**: Decoy systems designed to lure attackers, detect new threats, and gather intelligence.
* **Deception Technology**:
  + Uses automated, dynamic decoys.
  + Provides real-time alerts and reports for post-attack analysis.

**Firewalls**

* **Purpose**: Control and secure traffic between internal and external networks.
* **Characteristics**:
  + All traffic must pass through the firewall.
  + Only authorized traffic allowed.
  + Immune to penetration if configured correctly.
* **Capabilities**:
  + Monitors security events, supports VPNs, and enforces security policies.
* **Limitations**:
  + Cannot fully protect against insider threats or bypassed policies.

**Types of Firewalls**

1. **Packet Filtering**: Examines packets based on rules (e.g., IP, port, protocol).
2. **Stateful Packet Inspection**: Tracks connections for more context.
3. **Application Proxy**: Relays and filters application-level data.
4. **Circuit-Level Proxy**: Establishes secure TCP connections.

**Sandboxing**

* Isolates programs to prevent system-wide impact.
* Examples: Browser sandboxes (Google Chrome), Virtual Machines, Windows Sandbox.

**Penetration Testing**

* **Purpose**: Evaluate strengths of security controls.
* **Phases**:
  1. Information Gathering: Analyze domain, IP, DNS, and personnel data.
  2. Network Scanning: Discover live hosts, services, and vulnerabilities.
  3. Exploitation: Test vulnerabilities for severity.
  4. Reporting: Document findings and recommendations.
* **Testing Types**:
  1. **Black Box**: No information about the target.
  2. **White Box**: Full knowledge of the target.
  3. **Gray Box**: Partial information provided.