**INFORMATION SECURITY**

- Also known as InfoSec
- The practice of protecting information by mitigating information risks.
- A part of information risk management.
- Involves preventing or at least reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information.
- It also involves actions intended to reduce the adverse impacts of such incidents

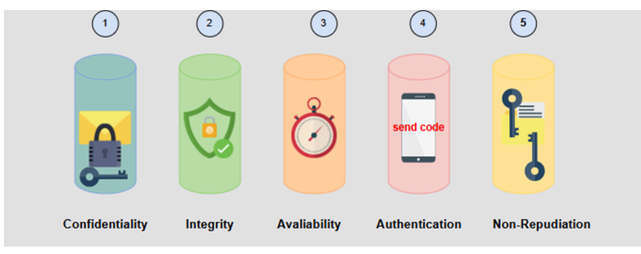
**CIA example: ATM**

- With two-factor authentication, confidentiality is addressed, and sensitive data is protected by using a debit card with a PIN code. This PIN code makes sure that only authorized individuals will have access to financial account information.
- ATMs and bank software help maintain data integrity by keeping records of all ATM transfers and withdrawals in a user's bank account. This helps ensure that information is accurate and up-to-date.
- ATMs are available (availability) for public use and are accessible at all times. This provides convenience and flexibility for users.

**INFORMATION ASSURANCE**

- Also known as IA
- The practice of assuring information and managing risks related to the use, processing, storage, and transmission of information. Information assurance includes the protection of the integrity, availability, authenticity, nonrepudiation, and confidentiality of user data.
- It encompasses not only digital protections but also physical techniques. These protections apply to data in transit, both physical and electronic forms, as well as data at rest.
- IA is best thought of as a superset of information security (i.e., umbrella term), and as the business outcome of information risk management.

**INFORMATION ASSURANCE FRAMEWORK**




1. **Confidentiality**
   - Assures that the unauthorized parties do not have access to information. The information that is being transmitted must be encrypted. Only those who are authorized can decrypt and access this information.
2. **Integrity**
   - Assures that the information remains in its original state, meaning the system should safeguard data's accuracy and completeness. Integrity ensures that unauthorized individuals do not tamper with or modify the information.
3. **Availability**
   - Ensures that the authorized parties have easy and timely access to the information system. This pillar ensures the system remains robust and fully functional even during adverse conditions. It involves protection against threats that can block access to the information system.
4. **Authentication**
   - Ensures the validity of a transmission or a message or the verification of a party's authorization to receive specific information. It prevents impersonation and requires confirmation of the identities of the parties before giving access to the information system and resources.
5. **Non-Repudiation**
   - Ensures that the sender is provided with proof of delivery and the receiver is provided with proof of the sender's identity. This attribute assures the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's sending the message so that neither can deny sending or receiving data, respectively.

**INFORMATION SECURITY: IS IT AN ART OR A SCIENCE?**

- Implementation of information security is often described as a combination of art and science
- "*Security artisan*" idea: based on the way individuals perceive systems technologists since computers became commonplace

- **AS AN ART**
  - No hard and fast rules, nor many universally accepted complete solutions
  - No manual for implementing security through entire system

- **AS SCIENCE**
  - Dealing with technology designed to operate at high levels of performance
  - Specific conditions cause virtually all actions that occur in computer systems
  - Nearly every fault, security hole, and system malfunction is a result of the interaction of specific hardware and software
  - If developers had sufficient time, they could resolve and eliminate faults
- **AS SOCIAL SCIENCE**
  - Social science examines the behaviour of individuals interacting with systems
  - Security begins and ends with the people who interact with the system
  - Security administrators can greatly reduce levels of risk caused by end users, and create more acceptable and supportable security profiles

---

**SECURING ORGANIZATION DATA**

**MCCUMBER CUBE**

- The McCumber Cube, developed by John McCumber in 1991, is a three-dimensional framework used in *Information Assurance (IA)* and *Information Security (InfoSec)*.
- It helps organizations ensure that security controls are complete, balanced, and systematic by examining security from three critical dimensions.

**Purpose:**

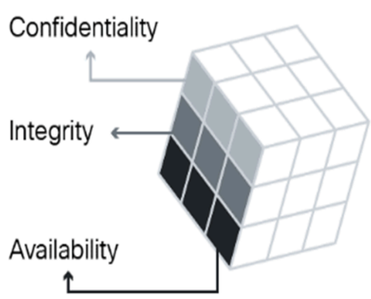
- To analyze security holistically
- To identify gaps in protection
- To guide policy, technical, and operational controls

**Application:**

- Used in risk assessment, security planning, audits, compliance, and academic instruction.

**DIMENSION 1: Defines what must be protected**

I. Foundational principles for protecting information systems




1. **Confidentiality**

Ensures that information is accessible only to authorized users.

**Application:**

- Access control
- Encryption
- Authentication mechanisms

**Example:**

Student records in a university database are accessible only to authorized faculty and registrars through username/password and role-based access.

2. **Integrity**

Ensures that information is accurate, complete, and not altered without authorization.

**Application:**

- Hashing
- Digital signatures
- Version control

**Example:**

Grades entered into a Learning Management System (LMS) are protected using audit logs to prevent unauthorized changes.

3. **Availability**

Ensures that information and systems are available when needed.

**Application:**

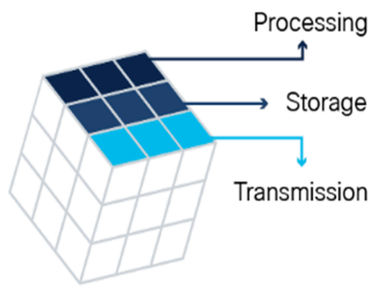
- Backups
- Redundancy
- Disaster recovery planning

**Example:**

A computer laboratory system uses regular backups and UPS devices to ensure systems remain accessible during power interruptions.

**DIMENSION 2: Identifies where information exists**

II. Protection of information in each of its possible states




1. **Data at Rest (Storage)**

Information is stored in databases, hard drives, USBs, or cloud storage.

**Application:**

- Disk encryption
- Secure storage policies

**Example:**
Research data stored on a university server is encrypted to protect it from unauthorized access.

2. **Data in Transit (Processing/Transmission)**

Information being transmitted across networks.
**Application:**
- Secure protocols (HTTPS, SSL/TLS)
- VPNs

**Example:**
Online enrollment systems use HTTPS to secure data transmitted between student devices and servers.

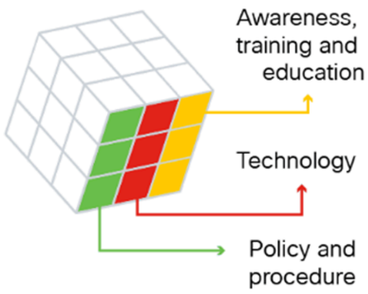
3. **Data in Use (Processing)**

Information currently being processed or accessed by users.
**Application:**
- Session management
- Endpoint security

**Example:**
A logged-in instructor accessing student grades on a lab computer is protected through automatic session timeouts.

**DIMENSION 3: Defines how protection is implemented**

III. Security measures used to protect data




1. **Policy and Practices (Administrative Controls)**

Rules, guidelines, and procedures governing system use.
**Application:**
- Acceptable Use Policy
- Data Privacy Policy
- Incident Response Plans

**Example:**
A computer laboratory policy prohibits the sharing of user accounts and outlines disciplinary actions for violations.

2. **Education, Training, and Awareness (Peopleware Controls)**

Ensures users understand their roles and responsibilities in security.
**Application:**
- Security training
- Awareness campaigns

**Example:**
Students receive orientation on the proper use of lab computers and data privacy compliance.

3. **Technology (Technical Controls)**

Hardware and software tools are used to enforce security.
**Application:**
- Firewalls
- Antivirus
- Intrusion detection systems

**Example:**
Computer laboratory machines are protected by endpoint security software and network firewalls.

**Applying the McCumber Cube in Practice**

1. Identify information assets
2. Map each asset across the three dimensions
3. Check if Confidentiality, Integrity, and Availability are addressed
4. Apply administrative, technical, and human controls for each data state
5. Identify gaps and implement controls

**Importance of the McCumber Cube**

1. Provides a complete security view
2. Prevents over-reliance on technology alone
3. Supports risk management and compliance
4. Ideal for academic and institutional environments

---

**INFORMATION SECURITY RISK MANAGEMENT**

- Also known as ISRM
- The process of managing risks associated with the use of information technology
- It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets
- The end goal of this process is to treat risks in accordance with an organization's overall risk tolerance.

**4 STAGES OF ISRM**

1. **IDENTIFICATION**

- **Assets**
  - These include physical equipment like servers, laptops, and mobile devices, and digital assets like data, software, and intellectual property
- **Threats**
  - Are actors or events that could exploit vulnerabilities and harm assets.
- **Vulnerability**
  - Are weaknesses present in assets that threats could exploit. Vulnerabilities can be technical (software bugs, security configuration flaws) or procedural (no strong password policy, lack of training).
- **Controls**
  - These are the measures that organizations implement to mitigate risks. They can be preventive, like *firewalls*, or detective, like *security monitoring* and *log reviews*.

2. **ASSESSMENT**

- **Risk Assessment**
  - The probability of the risk occurring, while the impact is the severity of the consequences if it does occur.
- **Prioritizing risks**
  - Not all risks are equal. Some are more likely to happen and have a greater impact. Prioritize risks so you can focus resources on mitigating the most critical.

Can be shown in the equation:

**Risk = Likelihood * Impact**

**RISK SCORING**

- First, assign a numeric value to each factor.

For example, you might assess the risk of a data breach as medium likelihood and high impact. Using a scale of 1 to 5, equates the likelihood to 3 and impact to 5, totaling 15.

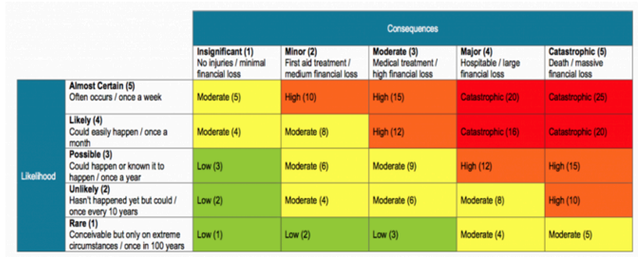
Note that risk scoring is not a precise science.
*"It is a way of comparing risks and prioritizing mitigation efforts. Your assigned values will depend on your risk appetite and tolerance."*

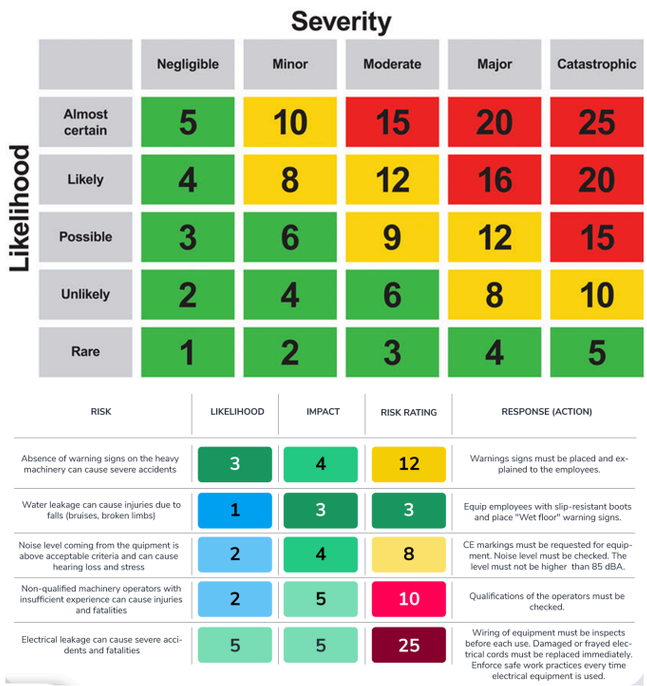
**A. Likelihood (How often it may occur)**

| Score | Level | Description |
|---|---|---|
| 1 | Low | Rare, unlikely to occur |
| 2 | Medium | Occasional, possible |
| 3 | High | Frequent or very likely |

**B. Impact (How serious the effect is)**

| Score | Level | Description |
|---|---|---|
| 1 | Low | Minimal disruption, easy to recover |
| 2 | Medium | Noticeable disruption, moderate recovery effort |
| 3 | High | Severe damage, data loss, safety or operational failure |

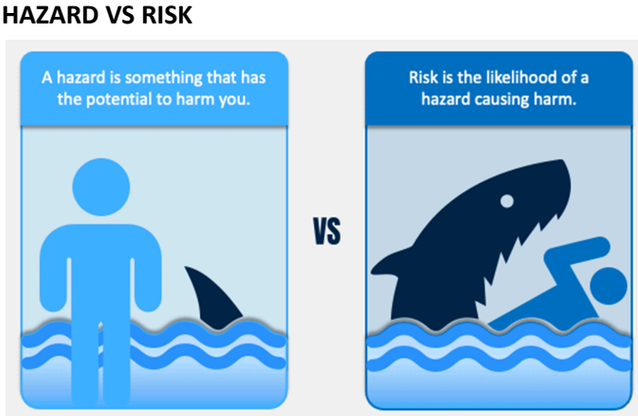


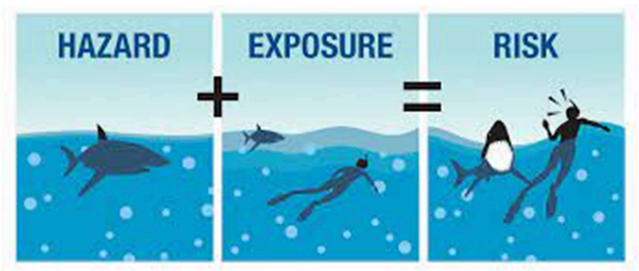







**HAZARD VS RISK**




---

**COMPUTER THREATS**

- Any potential danger that can exploit a vulnerability in a computer system, network, or information asset, resulting in unauthorized access, damage, disruption, or loss of data.
- Any circumstance or event with the potential to adversely impact system operations, assets, or individuals through unauthorized access, destruction, disclosure, modification of information, or denial of service. *(ISRM Definition)*

**HOW TO DETERMINE THREATS**

| Asset Identification | Vulnerability Analysis | Threat Source Identification |
|---|---|---|
| Identify what needs protection: | Determine weaknesses such as: | Threats may come from: |
| • Hardware (computers, servers, CCTV, routers)<br>• Software (OS, applications, databases)<br>• Data (student records, grades, research files)<br>• Peopleware (users, administrators) | • Outdated software<br>• Weak passwords<br>• Lack of access control<br>• Poor user awareness | • Internal users (students, staff)<br>• External attackers (hackers, malware authors)<br>• Environmental factors (fire, flood, power failure) |

**CATEGORIES OF COMPUTER THREATS**

**I. PEOPLEWARE**

A. Social Engineering
- Phishing
  - Spear Phishing
  - Whaling
  - Smishing (SMS Phishing)
  - Vishing (Voice Phishing)
- Pretexting
- Baiting
- Tailgating

B. Insider Threat

**II. HARDWARE**

*A. Processor / Chip Vulnerabilities*
- Spectre
- Meltdown
- Rowhammer
- Foreshadow
- ZombieLoad

*B. Physical Attacks*
- Evil Maid Attack
- Hardware Keylogger
- BadUSB
- Device Tampering
- Cold Boot Attack

**III. SOFTWARE**

*A. Malware*
- Virus
  - Brain
  - ILOVEYOU
  - Melissa
  - CIH (Chernobyl)
  - Michelangelo
- Worm
  - Morris Worm
  - Code Red
  - SQL Slammer
  - Conficker
  - Stuxnet
- Trojan Horse
  - Zeus (Zbot)
  - Emotet
  - TrickBot
  - Dridex
  - Redline Stealer
- Ransomware
  - WannaCry
  - LockBit
  - Ryuk
  - NotPetya
  - Jigsaw
- Spyware
  - Pegasus
  - FinFisher
  - CoolWebSearch
  - SpyNote
  - Keyloggers
- Rootkit (Stealth Software)
  - Sony BMG Rootkit
  - Kernel Rootkits
  - Bootkits
  - Firmware Rootkits
  - UEFI Rootkits

*B. Application / Web Attacks*

- Injection Attacks
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - XPATH Injection
  - NoSQL Injection
- Client-Side Attacks
  - XSS (Cross-Site Scripting)
  - Clickjacking
  - Drive-By Download
  - Malvertising
  - Browser Hijacking
- Watering Hole Attack

**IV. NETWORK**

*A. Denial of Service (DoS)*

- SYN Flood
- Ping of Death
- UDP Flood
- HTTP Flood
- Mirai Botnet

*B. Man-In-The-Middle (MITM)*

- Eavesdropping
- SSL Stripping
- Session Hijacking
- Rogue Access Point
- Evil Twin Attack

*C. Spoofing*

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Email Spoofing
- MAC Spoofing

**V. DATA & PRIVACY**

*A. Data Breaches*

- Yahoo Breach
- Equifax Breach
- Facebook Breach
- Marriott Breach
- Capital One Breach

*B. Identity-Based Attacks*

- Identity Theft
- Account Takeover
- Data Leakage
- Log Manipulation
- Privacy Invasion

**VI. MOBILE & IOT**

*A. Mobile Malware*

- Pegasus
- Spynote
- Joker Malware
- FluBot
- SMS Trojans

*B. IoT Attacks*

- Mirai Botnet
- Reaper Botnet
- BrickerBot
- Smart Device Hijacking
- IoT Exploits

**VII. INDUSTRIAL / CRITICAL INFRASTRUCTURE**

*A. Stuxnet*
*B. Triton / Trisis*
*C. Industroyer*
*D. BlackEnergy*
*E. Havex*

**VIII. ORGANIZATIONAL / STRATEGIC**

*A. Advanced Persistent Threats (APT)*

- APT29 (Cozy Bear)
- APT41
- Mustang Panda
- Fancy Bear (APT28)
- Lazarus Group

*B. Supply Chain Attacks*

- SolarWinds
- CCleaner
- ASUS ShadowHammer
- 3CX
- NotPetya

**IX. EMERGING / HYBRID**

*A. Deepfake Fraud*
*B. Cryptojacking*
*C. Zero-Day Exploits*
*D. AI-Powered Attacks*
*E. Disinformation Campaigns*

---

**ACRONYMS**

| | |
|---|---|
| CIA | – Confidentiality, Integrity, Availability |
| IA | – Information Assurance |
| ATM | – Automated Teller Machine |
| PIN | – Personal Identification Number |
| API | – Application Programming Interface |
| IS | – Information System |
| InfoSec | – Information Security |
| LMS | – Learning Management System |
| VPN | – Virtual Private Network |