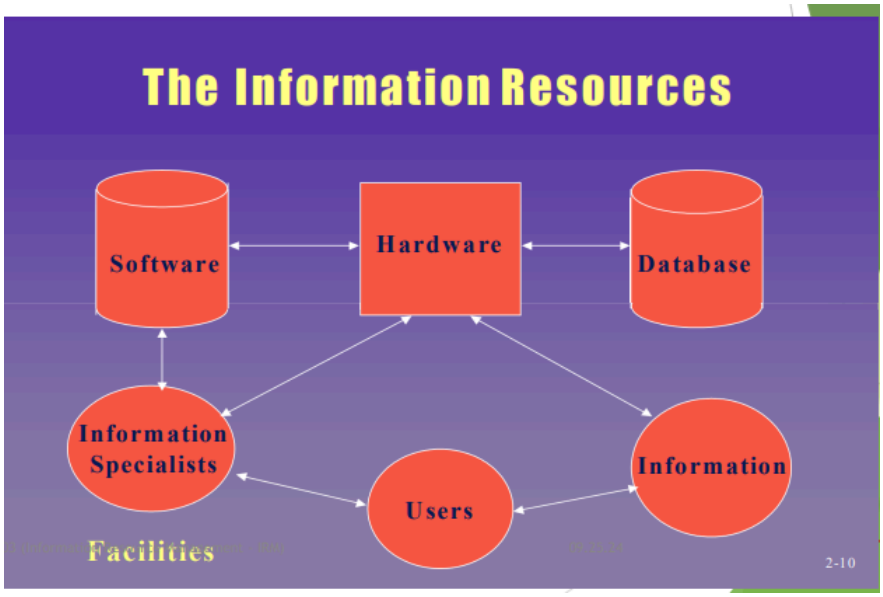
1. Information: is data that has been processed, organized, or structured in a way that gives it meaning and context.
2. Why information is needed (DPPC):
   - Decision making
   - Problem solving
   - Planning and strategy
   - Crisis management
3. Sources of information:
   - Internal Source: originates from within an organization. They provide data based on the organization's own data, processes, and personnel. Eg: Employee records, financial reports, sales data, etc.
   - External Source: originates from outside the organization. They provide a broader perspective. Eg: market research reports, news media, academic journals, etc.
4. Resources: refer to the various components and assets used to manage and support the effective processing, storage, retrieval, and dissemination of information within an organization.
5. To maximize the efficient and effective use of resources:
   - classify them for effective sharing and eliminate any unnecessary redundancies. Also, careful management is required to ensure that these resources are received, stored, and distributed correctly.
6. Management: is the process of planning, organizing, leading, and controlling resources eg. people, material, finance, etc to achieve an organizational goal effectively and efficiently.
7. IRM:
   - General Definition: is the strategic management of an organization's information assets effectively and efficiently.
   - Schneyman, 1985: the management of human and physical resources involved in the support of systems related to the development, enhancement, and maintenance of information.
   - McLeod and Brittain-White, 1988: the recognition of data and information as valuable resources and applying management principles used for physical resources to manage them.
   - Kerr, 1991: the belief that information is a valuable asset that should be rigorously managed to contribute to business success.
   - McLeod and Schell, 2001: an activity undertaken by managers at all levels of a firm to identify, acquire, and manage the information resources necessary to meet information needs.
8. Trauth (1989) on IRM states that: IRM concepts are based on the premise that information, related activities, technologies, and personnel are vital organizational resources that should be managed like any other resources in the organization.

9. Components of IRM in modern organization:



10. Why IRM: it ensures that an organization's information assets are effectively managed and utilized to enhance decision-making, drive efficiency, and achieve strategic objectives.

11. Benefits of IRM:

- Enhance decision making
- Increase efficiency
- Ensures data integrity, accuracy, and consistency
- Identifies and mitigates risks associated with information security

12. Who needs IRM: IRM is needed by any organization or individual that relies on data and information to make informed decisions, achieve their goals effectively, and be adaptive, knowing, and learning.

13. Adaptive organization: is one that easily adjusts to the changing needs of its stakeholders.

14. Knowing organization: is one that effectively gathers, shares, and uses knowledge to make informed decisions

15. Learning organization: is one that improves by encouraging its members to acquire new skills and knowledge.

16. Enterprise Resource Planning (ERP): is an integrated software used by organizations to manage and automate core business processes eg. human resource, supply chain, etc in a centralized system.

17. The Willard Model proposes implementing IRM by considering the following (CODEI):

- Identification: Finding and recording information resources in an inventory.
- Ownership: Establishing who is responsible for managing the information.
- Cost and value: Assessing the cost of an information resource and its value to the organization.

- Development: Enhancing the information resource to increase its value.
- Exploitation: Using the resource to generate further value, such as converting it into a saleable asset.

18. Information Warfare (IW): refers to the use of information and communication technologies to gain a competitive advantage in various domains e.g Technology.
19. Classes of IW:
    - Personal information warfare: refers to attacks targeting individuals to manipulate or exploit their personal data. Eg. phishing, doxing, astroturfing
    - Corporate information warfare: refers to conflicts between businesses over sensitive information. E.g. corporate espionage, data breaches, SEO manipulation
    - Global Information Warfare: refers to state-sponsored or large-scale actions aimed at manipulating or disrupting nations' information systems. E.g. Disinformation Campaigns, Election Interference, Social Media Manipulation
20. Corporate information warfare between kodak and fuji:
    - Fuji obtained Kodak's plans to create disposable cameras. Kodak employed former CIA operatives as “Information Warriors.” Ultimately, Kodak was the first to introduce the cameras to the market.
21. IT standards: are formal guidelines that establish best practices, procedures, and protocols for managing and utilizing technology within organizations or industries.
22. What requires standards:
    - Operating systems
    - Development languages
    - Telephony and conferencing
    - Peripherals
23. Consequences of not defining or enforcing standards:
    - System malfunction e.g. hardware and OS variations can cause crashes.
    - Security risk e.g. older OS versions may have exploitable vulnerabilities.
    - Budgetary impact e.g. Training on hardware and software can raise costs.
    - Business related issues e.g. Multiple financial systems can cause discrepancies.
24. Classes of standards:
    - Absolute standards: fixed models and systems used
      E.g. Dell OptiPlex PCs for workstations.
    - Non-standard standards: supported products but not required
      E.g. Adobe Photoshop as a supported application.
    - Special request standards: customized standards per specific needs
      E.g. Custom software developed for a specific project.
    - Don’t care: items with negligible operational impact
      E.g. generic USB flash drives with minimal impact.
    - Not allowed: prohibited products or technologies
      E.g. unauthorized peer-to-peer file-sharing software.

25. Criterias for selecting standards (FRMS):
    - Fitness for purpose
    - Reliability
    - Manageability
    - Scalability
26. benefits/ purpose of IT policies:
    - Provide a framework for effective IT management
    - Provide guidelines for approved hardware/ software
    - Provide procedures for user access control
    - Provide standards for asset usage and security reporting
27. Typical set of policies an organization must create:
    - Mobile security policy
    - IT security incident reporting policy
    - Email use policy
    - Password policy
    - BYOD policy
28. Steps to follow in enforcing standards:
    - Obtain senior IT/management approval and inform staff/ customers
    - Document standards and policies
    - Record rationale for the standards
    - Periodically redistribute standards with feedback
    - Regularly update standards
    - Apply a 'common sense' approach to approving standards
29. Service level agreement SLA: is a contract between the service provider and the service consumer in terms of when the service will be delivered, its quality, and scope.
30. Features of SLAs: must include -
    - Customer duties and responsibilities
    - Detailed fees and expenses
    - Disaster recovery procedures
    - Agreement termination clauses
31. Types of SLAs
    - Service to you from vendors or other service providers
        - ★ Equipment vendors guarantee response times, repair times, and parts replacement.
        - ★ Data centers provide assurances for power, cooling, temperature, humidity.
    - Service from you to your customers
        - ★ Focus on meeting or exceeding service levels
        - ★ Defines and manages user service expectations.
32. Benefits of SLAs:
    - Provides a bar that can deflect undue criticism

- Allows the business to manage the tradeoff between cost and speed
- Reduces the level of uncertainty the customer has with the process
- Tells the technical staff the minimum performance standards they must meet

33. IT Asset Management/ IT inventory management: integrates financial, contractual, and inventory functions to support lifecycle management and strategic IT decision-making.
34. Questions an asset management system should be able to answer:
    - How many devices are deployed enterprise-wide?
    - How many devices are deployed by site?
    - What is the total cost of deployed assets?
    - What is their current value?
35. From a process standpoint, asset Management is focused in three areas:
    - Physical inventory of devices: Essential for tracking assets, locations, and ownership for real-time infrastructure insights.
    - Contracts of finance: Controls IT spending and supports software compliance through financial integration.
    - Software compliance: Manages licensing and reduces costs through effective Software License Management.
36. Best practices for asset management:
    - Have a process owner
    - Ensure stakeholder alignment
    - Conduct internal audits
    - Set specific operational and financial goals
37. If an entity's information system security is compromised due to a lack of firewall or antimalware, it can result in:
    - System disruptions
    - Unauthorized access
    - Malware infections
    - Financial loss
38. Security: policies and measures to prevent unauthorized access, alteration, theft, or damage to information systems.
39. Controls: methods and procedures that ensure the safety of assets, accuracy of records, and adherence to management standards.
40. Why information systems are vulnerable:
    - Insider threats
    - Human error
    - Outdated software
    - Weak passwords
41. Site access controls: are security measures implemented to regulate who can enter a site, network, or system, and what resources they can access.

42. Purpose of site access controls: to limit access to secure areas, allowing only authorized individuals to enter.
43. Categories of controls/ security controls:
- Detective: identifies and alerts suspicious behavior e.g. logs, IDS
- Deterrent: discourages potential attackers by making threat of detection or punishment e.g. warning signs, CCTV
- Preventive: stops security incidents from happening by blocking or restricting actions: e.g. firewalls, encryption
- Corrective
- Recovery
- Compensating

44. Types of site access controls:
- Key card access systems
- Biometrics e.g. fingerprint, iris scan, retina scan
- Video surveillance
- Guard dogs
- Fences and walls
- Notices
- Exterior lighting

45. How a key card system works:
- User taps/swipes the card, which reads the card's number.
- Reader sends the number to the Key Card Controller.
- Controller checks the number in the Valid Key Cards Database.
- If valid, the door unlocks; if not, access is denied.
- Entry is logged in the Workstation, which manages records.

46. Advantages and disadvantages of key cards:
★ PROS
- Easy to use
- Easy to change access permissions
- Provides an audit record

★ CONS
- Can be use by others if lost
- Can become demagnetized over time
- Can be hacked or cloned

47. Advantages and disadvantages of metal keys:
★ PROS
- reliable backup when a key card system fails.
- Ideal for use in restricted areas, e.g. cabinets
- No electronic failure

★ CONS
- Easily duplicated

- Does not provide audit records
- Can be compromised using bump keys.

48. Duties of guards:
    - Verify employee IDs and manage visitors.
    - Inspect parcels and equipment in/out.
    - Oversee deliveries and detain suspicious individuals.
    - Provide assistance as needed.
49. Advantages of guards:
    - Immediate response
    - They use discretion effectively
    - Deterrence of crime
50. A security measure that serves as a detective, preventive, and deterrent control is: guard dogs
51. Examples of video surveillances:
    - CCTV Cameras - Dome Cameras - PTZ Cameras - IP Cameras
52. Physical controls:
    - Bollards - Crash gates
53. Secure siting: is the strategic placement of structures, facilities, or infrastructure to minimize risks and vulnerabilities.
54. Threat identification:
    ★ Natural e.g. flooding, earthquakes, volcanoes
    ★ Man-made e.g. chemical spills, transportation accidents, social unrest
55. Siting factors:
    - Building marking
    - Loading and unloading areas
    - Shared-tenant facilities
    - Nearby neighbors
56. Asset protection: refers to strategies and measures implemented to safeguard an individual's or organization's valuable assets from loss, theft, or damage.
57. Asset protection for laptop computers:
    - Anti-theft cables
    - Lockable laptop cabinets or safes
    - Strong authentication
    - Full encryption
58. Asset protection for servers and backup media:
    - Locked server rooms
    - Off-site storage for backup media
    - Intrusion detection systems
    - RBAC (role based access control)
59. Asset protection for sensitive documents:
    - Fireproof and waterproof safes

- Document shredding
- Encryption
- DRM (digital rights management)

60. Asset protection for damage protection:
    - Install sump pumps or barriers in flood-prone areas.
    - Install automatic fire detection.
    - Implement maintenance schedules for critical systems.
61. Asset protection for fire protection:
    - Install smoke detectors throughout the facility
    - Install automatic fire sprinkler systems.
    - Inspect electrical systems and appliances for fire hazards.
62. Cabling security:
    - ★ On-premises:
        - Place cabling inside conduits
        - Route cables away from exposed areas
    - ★ Off-premises:
        - Implement diverse and redundant network routing
        - Utilize encryption for data transmitted over the network
63. Types of attacks:
    - Denial of service
    - Ping flood
    - Botnets
    - Malicious code (e.g. viruses, trojan horses, w0rms, etc)
64. Denial of service attack (DOS): is a cyberattack aimed at disrupting the normal operations of a network, system, or servers by overwhelming it with excessive traffic or malicious requests.
65. Note that: any kind of attack that renders its victim unable to perform normal activities is a DoS.
66. Ping flood: is a type of DoS attack that involves overwhelming a target network or system with excessive ICMP echo requests (pings) making it unresponsive.
67. Note that: ping flood can be very effective when launched by zombies within a botnet as a DDoS attack.
68. ICMP stands for: Internet Control Message Protocol.
69. Managing ping floods:
    - Blocking ICMP traffic
    - Use firewalls or access control
    - Implement packet filtering rules
70. Botnets: are networks of compromised computers (zombies) or devices that are controlled remotely by an attacker.
71. Bot herder: is a person who remotely controls and manages a botnet.

72. Note that: computers often join a botnet after being infected with some type of malicious code or software.
73. Managing botnets:
    - Ensure anti-malware is running and updated.
    - Keep browsers and plug-ins up-to-date.
    - Avoid disabling built-in browser security features.
74. Malicious code: is any script or program designed to harm or damage computer systems or networks.
75. Forms a malicious code can take:
    - Viruses
    - Worms
    - Trojan horses
    - Logic bombs
76. Malicious code is often called: a malware
77. The most common form of security breach today is: malicious code
78. Types of malicious code attacks:
    - Viruses
    - Trojan horse
79. Computer viruses have two main functions:
    - Propagation: refers to the virus's ability to replicate itself and spread through systems.
    - Destruction: refers to the malicious actions taken by the virus once it has infected a system.
80. Reason why very few viruses attack UNIX, Ubuntu, Mac, etc OS:
    - Diverse Unix OS versions reduce uniform virus targets.
    - Independent designs by multiple developers increase security.
81. Antivirus mechanisms:
    - Signature-based detection:
    - Heuristic-based mechanism:
82. Signature-based detection:
    - involves creating unique digital signatures for known malware. When a file or program is scanned, its signature is compared to the database of known malware signatures. If a match is found, the file is flagged as malicious.
83. Actions taken by signature-based detection:
    - Removes virus to disinfect files and restore system safety.
    - May quarantine the file to allow manual review by user or admin.
    - May delete high-risk files for system security.
84. Warnings about signature-based detection:
    - Effectiveness relies on up-to-date virus definitions.
    - Frequent updates are needed to detect new viruses.
    - Outdated definition files quickly weaken defenses.

85. heuristic-based mechanism:
- involves examining a file's behavior and characteristics to identify suspicious patterns. This method looks for anomalies like unusual file modifications, network activity, or attempts to self-replicate.

86. Access Control Attack: is a cyberattack that aims to bypass or exploit vulnerabilities in an organization's access control mechanisms.

87. Access control attack objectives:
- Guess credentials
- Malfunction of access controls
- Bypass access controls
- Replay known good logins
- Trick people into giving up credentials

88. Buffer Overflow: is security vulnerability that occurs when a program writes more data to a buffer than it can hold.
- Countermeasure:
    - ★ “safe” coding that limits length of input data

89. Script Injection: is a cyberattack where an attacker inserts malicious code into a web application.
- Countermeasure:
    - ★ strip “unsafe” characters from input

90. Server-side script injection
- SQL injection:

91. Client-side script injection
- Cross site scripting
- Cross site request forgery

92. Data Remanence: refers to the residual representation of digital data that remains after attempts to erase or remove it.
- Countermeasure:
    - ★ Improve media physical control.

93. Denial of Service countermeasure:
- Input filters
- Patches
- High capacity

94. Dumpster Diving: refers to the act of searching through company trash or discarded items to find sensitive information.
- Countermeasure:
    - ★ On-site shredding

95. Eavesdropping: refers to the act of secretly listening to private communication to gather sensitive information.
- Countermeasures:
    - ★ encryption

96. Eavesdropping methods:
    - Wiretapping - Packet Sniffing - Man-in-the-middle attacks

97. Emanations (electromagnetic eavesdropping): refers to the interception of unintentional electronic signals from devices to extract information.
    - Countermeasures:
        ★ Shielding

98. Spoofing and Masquerading: refers to when attackers impersonate another entity to gain unauthorized access or deceive a target.
    - Countermeasure:
        ★ Strong authentication - MFA

99. Social engineering: refers to when an attacker manipulates or deceives people into revealing confidential information or performing certain actions.
    - Countermeasure:
        ★ Security awareness training

100. Phishing: is a type of social engineering attack where an attacker impersonates a legitimate entity to deceive people into sharing sensitive information e.g passwords, credit card number, etc.

101. Pharming: refers to when an attacker redirects users from a legitimate website to a fraudulent one without their knowledge.

102. Password guessing: refers to when attackers try various combinations of characters to figure out a user's password and gain unauthorized access to their account or system.
    - Countermeasure:
        ★ Aggressive password policy

103. Password Cracking: refers to the process of attempting to decipher a password to gain unauthorized access to a system or account.
    - Countermeasure:
        ★ Frequent password changes

104. War dialing: is an attack where an automated software is used to dial numerous phone numbers to find vulnerable modems or systems to exploit.

105. Sabotage: refers to intentional acts of damaging or disrupting an organization's operations, systems, or processes to cause harm or loss.

106. Espionage: refers to the practice of spying or gathering secret information, often targeting government, military, or corporate secrets.

107. Document disposal procedures:
    - data wiping
    - Shredding
    - Pulverizing
    - Incineration

108. Risk: is the possibility that a threat will exploit a vulnerability to cause harm to an information system asset.

109. Risk management: refers to the process of developing a strategy to ameliorate appropriate individual risks until the overall level of risk is reduced to an acceptable level.

110. Steps/ approaches to risk management are:

- Risk Assessment
  - Types: Qualitative risk assessment, Quantitative risk assessment
- Risk Treatment

111. For a given scope of assets in a qualitative risk assessment, identify the:

- Vulnerabilities: weaknesses or flaws in a system
- Threats: potential events or entities that could cause harm
- Threat probability: likelihood that a specific threat will exploit a vulnerability
- Impact: the extent of damage or loss that could result if a threat materializes
- Countermeasures: strategies implemented to reduce vulnerabilities, mitigate threats, or lessen their impact.

112. Metrics of each risk in a quantitative risk assessment:

- Asset value: replacement cost and/or income derived through the use of an asset.
- Exposure factor (EF): portion of asset's value lost through a threat.
- Single Loss Expectancy (SLE) = Asset($) × EF(%)
- Annualized Rate of Occurrence (ARO): probability of loss in a year(%).
- Annual loss expectancy (ALE) = SLE × ARO

113. Example of qualitative risk assessment:

Threat	Impact	Initial Probability	Counter-measure	Residual Probability
Flood damage	H	L	Water alarms	L
Theft	H	L	Key cards, surveillance, guards	L
Logical intrusion	H	M	Intrusion prevention system	L

114. Example of a quantitative risk assessment:

✓ Theft of a laptop computer, with the data encrypted

- Asset value: $4,000
- Exposure factor: 100%
- SLE = $4,000 x 100% = $4,000
- ARO = 10% chance of theft in a year
- ALE = 10% x $4,000 = $400

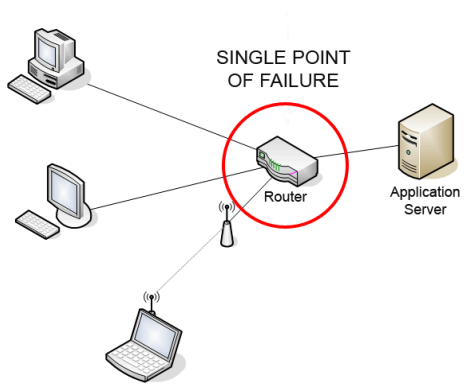
115. Several ways of risk treatment(response):
- Risk acceptance: Acknowledge the risk and its consequences.
- Risk avoidance: Eliminate the risk by not engaging in the activity causing it.
- Risk reduction: using countermeasures to reduce risks.
- Risk transfer: shift the risk to a third party, typically via insurance.

116. Residual risk: the remaining risk that persists after risk treatment measures.

117. CIA triad: represents the three core principles of information security.
- Confidentiality: Ensuring information is accessible only to authorized individuals.
- Integrity: Ensuring the accuracy and trustworthiness of information.
- Availability: Ensuring information and systems are accessible when needed.

118. Defense in Depth: refers to a security strategy that uses multiple layers of defense (technical, physical, and administrative controls) to protect assets. It reduces the risks from:
- Vulnerability of a single device
- Malfunction of a single device
- Fail open of a single device

119. Single Point of Failure(SPOF): is a component or part of a system that, if it fails, would cause the entire system to fail.



120. When a security mechanism fails, there are usually two possible outcomes:
- Fail open: the mechanism permits all activity
- Fail closed(Fail secure): the mechanism blocks all activity.

121. Privacy: is the protection and proper handling of sensitive personal information.

122. Issues related to privacy:
- inappropriate uses
- unintended disclosures to others

123. Personally identifiable information (PII):
- Name
- SSN
- Phone number
- Drivers license number

- Credit card numbers.