Ch.5 summary By @MHazazi

Information Assets and Systems

- **Information Assets**

  Any information item, regardless of storage format, that represents value to the organization Customer data, employee records, IT information, reputation, and brand.

- **Information system**

  A way and a place to process, store, transmit, and communicate the information. Usually a combination of both hardware and software assets Can be off-the-shelf or customized systems

  - off-the-shelf system = Any organization can use it
    - Pros= Cheaper, ready to use
    - Cons= Might come with unwanted features, hard to add new features
  - customized systems = depend on organization requirement
    - Pros= fulfil all requirements, easy to update
    - Cons= expensive, development time consumption

- **Information Ownership**
  - ISO stands for information security officer
  - The ISO is accountable for the protection of the organization.

- **information owner** responsible for information he owns
- **information custodian** responsible for implementing actual controls protect information assets
  - The ISO is the central repository of security information

Information Classification

- **Information Classification**
  - organization of information assets according to their sensitivity to disclosure
- **Classification Systems**
  - labels that we assign to identify the sensitivity levels

1) Federal Information Processing Standard 199 (FIPS-199) requires information owners to classify information and information systems based on CIA criteria as:

- Low potential impact
- Moderate potential impact
- High potential impact

2) Government & Military Classification Systems:

- **Top Secret (TS)** = information if it was disclosed it will cause grave damage
- **Secret (S)** = information if it was disclosed it will cause serious damage
- **Confidential (C)** = information if it was disclosed it will cause damage
- **Unclassified (U)** = information disclosed to public without any threat to national interest
- **Sensitive But Unclassified (SBU)** = information if it was disclosed it might adversely affect

3) Commercial classification systems:

- No standard: Each company can choose its own system that matches its culture and needs
- Usually less complex than the government system
- The more regulated a company, the more complex the classification system it adopts
- **Most systems revolve around these four classification levels:**
  - **Protected** = Data protected by law, regulation
  - **Confidential** = Data essential to the mission of an organization , available to a small authorized individuals , Disclosure would cause significant financial loss, reputation loss and legal liability.
  - **Internal Use** = Data about ordinary company business. Disclosure would impair the business and lead to business, financial, or legal loss
  - **Public** = Data doesn't need protection , intended for public.

What is NPPI ?

Non-public personal information (NPPI) is data or information considered to be personal in nature, subject to public availability. if disclosed is an invasion of privacy.

Reclassification/Declassification

- The need to protect information may change
- As result, the label assigned to that information may change as well
- Downgrading sensitivity levels = **declassification**
- upgrading sensitivity levels = **reclassification**

Labeling and Handling Standards

- **Information labeling:**
  - Labeling assigned classification to information custodians and users
  - Labels must be clear and self-explanatory
  - In electronic form, the label should be made part of the filename
  - In printed form, the label should be clearly visible on the outside and in the header/footer

- **Information handling:**
  - Information must be handled in accordance with its classification
  - information user is responsible for using information in accordance with classification level

Information Systems Inventory

- Many organizations don't have an up-to-date inventory
- Creating a comprehensive inventory of information systems is a major task
- Both hardware and software assets should be inventoried
- Each asset should have a unique identifier and a description
- Company assets should be accounted for at all times
- An asset management procedure should exist for moving and destroying assets

- **Hardware assets include (but are not limited to):**
  - Computer equipment
  - Printers
  - Communication and network equipment
  - Storage media
  - Infrastructure equipment

- **Software assets include (but are not limited to):**
  - Operating system software
  - Productivity software
  - Application software