Cybersecurity

Data Sovereignty and Protection

CYBER.ORG

Data Sovereignty

- Data has to follow laws
  - Location matters
  - Must be compliant
    - Local and federal laws
- Becomes important with cloud computing
  - Data stored in one location
  - Data edited/viewed in another location

Data Loss Prevention (DLP)

- Prevent third-parties from accessing sensitive data
  - Data “leakage”
- Many sources of data, many destinations for it to go
  - Multiple threats require multiple solutions
- Scan for keywords related to fraud or sensitive data loss
  - Emails messages
  - Attachments
  - Web traffic

DLP techniques

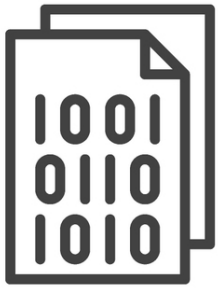
- Prevent USB storage devices on computers
  - No thumb drives, external hard drives, SD card readers, etc.
- Cloud-based DLP
  - Filtering which files go into/out of cloud
  - Monitoring sharing and access rights
- Email DLP
  - Filtering, limiting attachment types
  - Prevent confidential internal emails from going external
  - Prevent attachments from going to personal email accounts
  - Prevent forwarding or Reply-All on emails with sensitive info
  - Prevent fraudulent emails (esp. phishing attacks)

Encryption

- Masking
  - Make data unclear, different from original
  - Hard to read/decipher
- Encryption
  - Plaintext - original message
  - Ciphertext - encrypted message
  - Encrypt - going from plaintext to ciphertext
  - Decrypt - going from ciphertext to plaintext

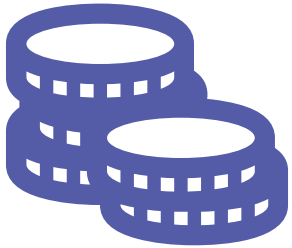
States of Data

- Data-in-use (processing)
  - On the computer
  - Being accessed
  - Being processed
- Data-in-motion (transit)
  - On the network
  - In transit
- Data-at-rest
  - On a drive
  - On a server
  - Stored for later access or transmission



Tokenization and Rights Management

- Tokenization
  - Process of turning sensitive data into non-sensitive data
  - Process cannot be reversed



- Rights Management
  - Forms of information control
  - Examples:
    - Information Rights Management (IRM)
    - Enterprise Rights Management (ERM)
    - Digital Rights Management (DRM)