CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-8-data_security_and_privacy_practices
Title: Data Security and Privacy Practices
Subtitle: CompTIA Security+ (SY0-501)

5.8 Data Security and Privacy Practices

- 5.8 Given a scenario, carry out data security and privacy practices.
  - Data destruction and media sanitization
    - Documents
      - NIST 800-88r1(Guidelines for Media Sanitization)
      - DoD 5220.22-M(Media Sanitization Guidelines)
    - Data Sanitization
      - NIST 800-88 Defines sanitization as "the process to render access to target data on the media infeasible for a given level of recovert effort
      - Categories for actions taken to sanitize media
        - Clear
          - Basic formatting for non-invasive recovery techniques
        - Purge
          - Applies physical/logical techniques that renders target data recovery infeasible with state of the art laboratory techniques
        - Destroy
          - Renders target data recovery infeasible with state of the art laboratory techniques with no ability to use the media to continue to store data
    - Burning
      - Destroys the target data as will
    - Shredding
      - Destroys the target data, including flexible media
      - Irreversible file destruction
    - Pulping
      - Pulping can be done mechanically or or cemically
    - Pulverizing
      - A destroy sanitization technique that completely eradicates the data and the media
    - Degaussing
      - A purging sanatization technique that uses high powered magnets to eradicate the data
      - Care shoud be taken when deqaussing flash-based storage as areas of the SSD use non-volatile NON-MAGNETIC media
    - Purging|(mentioned as one of the three sanatization techniques)
    - Wiping
      - Data overwriting
      - Unlike deguassing, which renders the media unusable
    - Secure Erase is a protocol that can be built into the drive
    -
  - Data sensitivity labeling and handling
    - Confidential
      - For use within the company only
      - Unauthorized disclosure could have a serious affect on the company
      - Examples
        - Trade Secrets
        - HIPPA Information
        - PII
        - PCI DSS information
    - Private
      - Personal information for use inside the company
      - Disclosure could adversely affect an individual employee or the company as a whole

        - Public
            - Basic attempts are made to openly disclose the information
            - Will not adversely effect the company or employees
        - Proprietary
            - Trade secrets
            - Programming Code
        - PII
            - Information that is used to identify an individual
            - Social Security, phone numbers, address, employee information, salary
        - PHI
            - Protected Health Information
            - Health status, payment/balance for healthcare
    - Data roles
        - Owner
            - ensures that the maintenance or contractual agreements are in place and are sufficent in protecting the confidentiality commensurate with the impact of information disclosure
        - Steward/custodian
            - Should ensure that appropriate supervision of onsite media maintenance by service providers occurs, when necessasry. Information owner/steward should fully understand the sensitivity of the information under their control
        - Privacy officer
            - The privacy officer is responsible for providing advice regarding the privacy issues surrounding the disposition of privacy information and the media upon which it is recorded.
    - Data retention
        - Usually defined in a company's data retention policy
        - HIPPA, Sarbanes-Oxley Act (SOX), PCI DSS
    - Legal and compliance