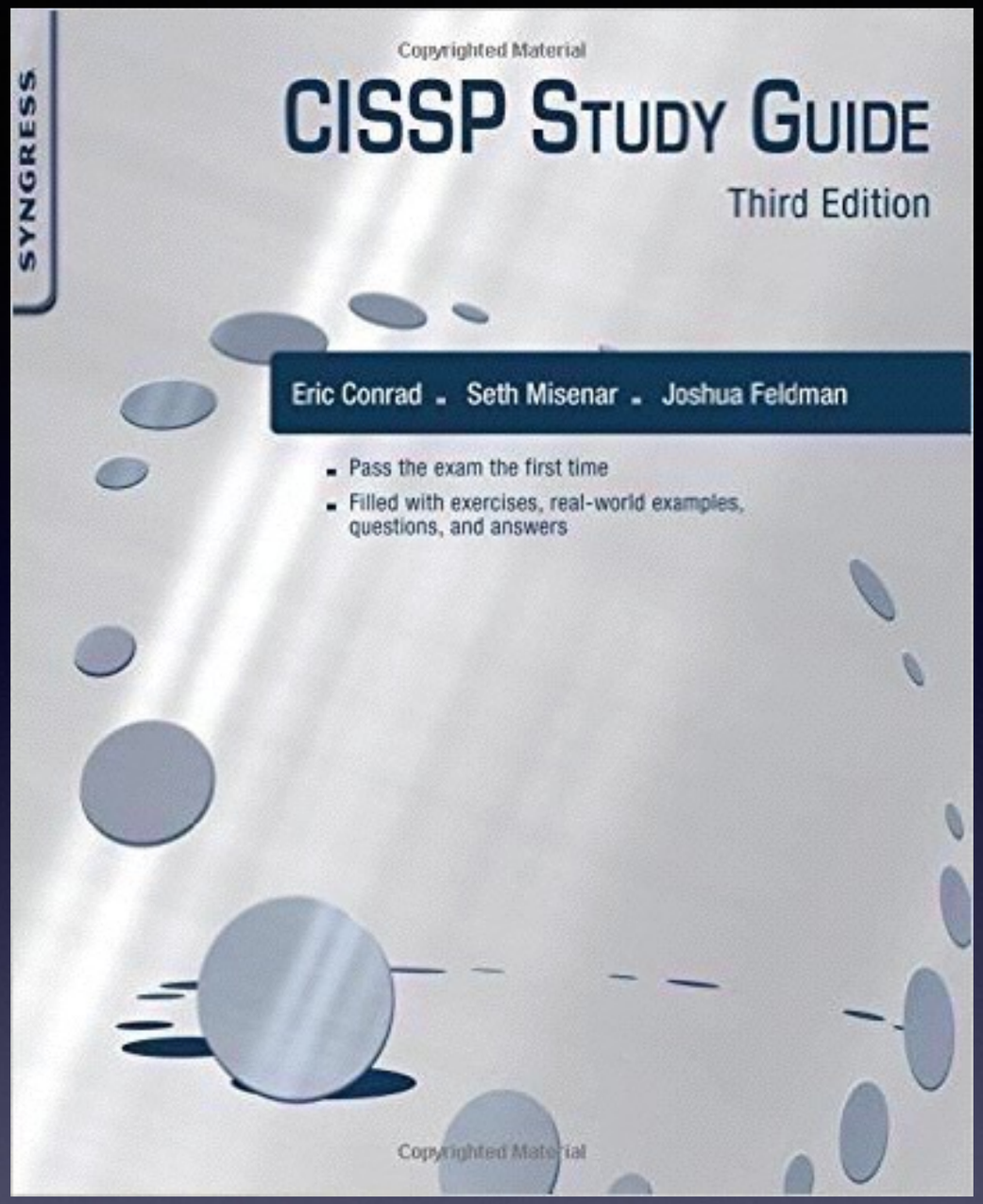
CNIT 125: Information Security Professional (CISSP Preparation)



Ch 3. Asset Security

Classifying Data

Labels

- **Governments**
  - **Confidential, Secret, Top Secret**
    - **Threats to national necurity**
  - **SBU (Sensitive But Unclassified)**
    - **Sensitive but not a matter of national security, like employee health records**
  - **For Official Use Only (FOUO)**
- **Private Sector**
  - **"Internal Use Only", "Company Proprietary"**

Security Compartments

- **Sensitive Compartmented Information (SCI)**
  - **Highly sensitive information**
  - **Examples (not testable)**
    - **HCS, COMINT (SI), GAMMA (G), TALENT KEYHOLE (TK)**
- **Compartments require a documented and approved need to know in additional to a normal clearance such as top secret**

Clearance

- **Formal determination whether a user can be trusted with a specific level of information**
  - **Considers both current and future potential trustworthiness**
  - **Issues: debt, drug or alcohol abuse, personal secrets**
  - **Most common reasons for denying clearance**
    - **Drug use and foreign influence**

Formal Access Approval

- **Documented approval from the data owner for a subject to access certain objects**
- **Requires the subject to understand all the rules and requirements for accessing data**
- **And consequences if the data is lost, destroyed, or compromised**

Need to Know

- **Most systems rely on least privilege**
- **Rely on users to police themselves by following policy and only attempting to access information they need to know**

Sensitive Information/Media Security

- **Sensitive Information**
  - **Requires protection**
  - **Resides on media**
    - **Primary storage and backup storage**
- **Policies must cover**
  - **Handling**
  - **Storage**
  - **Retention**

Ownership

Business or Mission Owners

- **Senior management**
- **Create information security program**
- **Ensure that it is properly staffed, funded, and given organizational priority**
- **Responsible for ensuring that assets are protected**

Data Owners

- **Also called "information owner"**
- **Management employee responsible for ensuring that specific data is protected**
- **Determine sensitivity labels and frequency of backup**
- **Data owner does management**
- **Custodians perform actual hands-on protection of data**
- ***NOTE: this is different from the "Owner" in a Discretionary Access Control system***

System Owner

- **Manager responsible for the physical computers that house data**
- **Hardware, software, updates, patches, etc.**
- **Ensure physical security, patching, hardening, etc.**
- **Technical hands-on responsibilities are delegated to Custodians**

Custodian

- **Provides hands-on protection of data**
- **Perform backups, patching configuring antivirus software, etc.**
- **Custodian follows detailed orders**
- **Does not make critical decisions on how data is protected**

Users

- **Must comply with policies, procedures, standards, etc.**
  - **Must not write doen passwords or share accounts, for example**
- **Must be made aware of risks, requirements, and penalties**

Data Controller and Data Processors

- **Data Controllers**
  - **Create and manage sensitive data**
  - **Human Resources employees are often data controllers**
- **Data Processors**
  - **Manage data on behalf of data controllers**
  - **Ex: outsourced payroll company**

Data Collection Limitation

- **Organizations should collect the minimum amount of sensitive data that is required**

Memory and Remanence

Data Remanence

- **Data that remains on storage media after imperfect attempts to erase it**
- **Happens on magnetic media, flash drives, and SSDs**

Memory

- None of these retain memory for long after power is shut off
- RAM is main memory
- Cache memory
  - Fast memory on the CPU chip (level 1 cache) or
  - On other chips (Level 2 cache)
- Registers
  - Part of the CPU

RAM and ROM

- **RAM is *volatile***
  - **Data vanishes after power goes off**
- **ROM is not volatile**
- **Cold Boot Attack**
  - **Freezing RAM can make the data last longer without power, up to 30 min. or so**

DRAM and SRAM

- **Static Random Access Memory (SRAM)**
  - **Fast and expensive**
- **Dynamic Random Access Memory (DRAM)**
  - **Slower and cheaper**

Firmware

- **Small programs that rarely change**
  - **Ex: BIOS (Basic Input-Output System)**
- **Stored in ROM chips**

Types of ROM Chips

- **PROM (Programmable Read Only Memory) -- write-once**
- **Programmable Logic Device (PLD)**
  - **Field-programmable**
  - **Types include**
    - **EPROM (Erasable Programmable Read Only Memory)**
    - **EEPROM (Electrically Erasable Programmable Read Only Memory)**
    - **Flash Memory**

Flash Memory

- **USB thumb drives**
- **A type of EEPROOM**
- **Written by sectors, not byte-by-byte**
- **Faster than EEPROMs**
- **Slower than magnetic disks**

Solid State Drives (SSDs)

- **Combination of EEPROM and DRAM**
- **SSDs use large block sizes**
- **Blocks are virtual; the computer doesn't know the physical location of the blocks**
- **Bad blocks are replaced silently by the SSD controller**
- **Empty blocks are erased by the controller in a "garbage collection" process**

Cleaning SSDs

- **Overwriting data from the computer is ineffective**
  - **Cannot access all the blocks**
- **The SSD controller may have an ATA Erase command**
  - **But there's no way to verify its work**
  - **It makes no attempt to clean "bad" blocks**

Two Ways to Securely Erase an SSD

- **Physically destroy the drive**
- **Turn on encryption before the drive is ever used**
  - **That ensures that even the bad blocks are encrypted**
- **To erase it, delete the key**
- **iPhones work this way**
- **Proven effective in practice**

Data Destruction

Overwriting

- **Deleting a file does not erase its contents**
- **You must write on top of the sectors it used**
- **Also called *shredding* or *wiping***
- **A single pass is enough for a magnetic hard drive**

Degaussing

- **Exposing a magnetic disk or tape to high magnetic field**
- **Can be a secure erase if performed properly**

Destruction

- **Physically destroy the storage media**
- **More secure than overwriting**
- ***Paper shredders* destroy printed data**

Determining Data Security Controls

Certification and Accreditation

- **Certification**
  - **A system meets the requirements of the data owner**
- **Accreditation**
  - **Data owner accepts the certification**

Standards and Control Frameworks

- **PCI-DSS**
- **OCTAVE**
  - **Operationally Critical Threat, Asset, and Vulnerability Evaluation**
  - **From Carnegie Mellon U**
- **ISO 27000 Series**
  - **Used to be ISO 17799**
  - **International standard, very detailed and expensive to implement**

Standards and Control Frameworks

- **COBIT**
  - **Control Objectives for Information and related Technology**
  - **From ISACA (Information Systems Audit and Control Association)**
  - **A governance model**
- **ITIL**
  - **Information Technology Infrastructure Library**
  - **Framework for IT service management**

Scoping and Tailoring

- **Scoping**
  - **Determining which portions of a standard an organization will use**
  - **If there's no wireless, wireless is "out of scope"**
- **Tailoring**
  - **Customizing a standard for an organization**
  - **Controls selection, scoping, and compensating controls**

Protecting Data in Motion and Data at Rest

Drive and Tape Encryption

- **Protect data at rest, even after physical security is breached**
- **Recommended for all mobile devices and mobile media**
- **Whole-disk encryption is recommended**
- **Breach notification laws exclude lost encrypted data**

Media Storage and Transportation

- **Store backup data offsite**
- **Use a bonded and ensured company for offsite storage**
  - **Secure vehicles and secure site**
- **Don't use informal practices**
  - **Like storing backup media at an employee's house**

Protecting Data in Motion

- **Standards-based end-to-end encryption**
  - **Like an IPSec VPN**