**Chapter 5: Protecting Security of Assets**

To protect information, it is crucial to classify data. Any unclassified information is considered to be sensitive and may cause damage

.

US government uses the following classification

* **Top Secret** - information, the unauthorized disclosure of which can cause exceptionally grave damage to the national security
* **Secret** - can cause severe damage
* **Confidential** - can cause damage
* **Unclassified** - information that does not fall under other classifications and is usually publicly available

Although there is no standard, non-government bodies commonly uses the below classification

* Confidential/ Proprietary - exceptionally grave damage to organization
* Private - serious damage
* Sensitive - damage (any data which is neither public nor classified)
* Public - no damage

Data loss prevention (DLP) systems attempt to detect and block data exfiltration attempts. There are two primary types of DLP systems:

* Network-Based DLP - deployed on edge of the network and scans all outgoing data
* Endpoint-Based DLP  - deployed on endpoints and scans file system to block copy or print jobs

Classified data must be sanitized properly when not required. Sanitization refers to the destruction of media or using a trusted method to purge classified data from the media without destroying it.

Data remanence is the data that remains on media after the data was supposedly erased.

Common Data Destruction Methods

* **Erasing** media is simply performing a delete operation against a file. The actual data remains on the drive.
* **Clearing**, or overwriting, is a process of preparing media for reuse and ensuring that the cleared data cannot be recovered using traditional recovery tools. Spare sectors on hard drives, sectors labeled as “bad,” and areas on many modern SSDs are not necessarily cleared and may still retain data.
* **Purging** is a more intense form of clearing that prepares media for reuse in less secure environments. It provides a level of assurance that the original data is not recoverable using any known methods.
* **Degaussing** creates a strong magnetic field that erases data on magnetic media. It is used during the purging process for magnetic disks. It has no effect on SSDs, CDs, or DVDs.
* **Destruction** is the final stage in the life cycle of media and is the most secure method of sanitizing media.

Cryptographic erasure or crypto-shredding destroys cryptographic keys to ensure data becomes unusable even if the storage media gets lost or stolen.

Data Protection Methods

* **Digital Rights Management (DRM)** - attempts to provide copyright protection for copyrighted works using software based licenses, Persistent online authentication, automatic expiration, continuous audit trail, etc.
* **Cloud Access Security Broker (CASB)**- software placed logically between users and cloud-based resources to monitor and enforce administrator defined security policies.
* **Pseudonymization** - using pseudonyms to represent other data
* **Tokenization** - Tokenization is the use of a token, typically a random string of characters, to replace other data. It is often used with credit card transactions.
* **Anonymization** - Removing PII data from real data in an attempt to anonymize the information

Data processor is a natural or legal entity which processes personal data solely on behalf of the data controller.

Data controller is the person or entity that controls the processing of the data. The data controller decides what data to process, why this data should be processed, and how it is processed.

Companies that violate privacy rules in the GDPR may face fines of up to 4 percent of their global revenue.

The GDPR has mandated the role of a data protection officer for any organization that must comply with the GDPR.

The data owner is the person who has ultimate organizational responsibility for data. The owner is typically the chief executive officer (CEO), president, or a department head (DH).

The data owner is the person responsible for classifying data.

Data owners often delegate day-to-day tasks to a data custodian. A custodian helps protect the integrity and security of data by ensuring that it is properly stored and protected.

Tailoring refers to modifying the list of security controls within a baseline to align with the organization’s mission.

Scoping is a part of the tailoring process and refers to reviewing a list of baseline security

controls and selecting only those controls that apply to the IT systems you’re trying to protect.