Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 5 of the official CISSP study guide. Here are the top things you need to know from this chapter on protecting the security of assets.

Understand the importance of data and asset classifications. Data owners are responsible for defining data and asset classifications and ensuring that data and systems are properly tagged. Additionally, data owners define requirements to protect data at different classifications such as encrypting sensitive data at rest, in transit and in use.

Data classifications are typically defined within security policies or data policies. Define PII and PHI. Personally identifiable information PII is any information that can identify an individual. Protected health information, PHI is any health related information that can be related to a specific person and in the US is subject to HIPAA.

Many laws and regulations mandate the protection of PII and PHI. Know how to manage sensitive information. Sensitive information is any type of classified information and proper management helps prevent unauthorized disclosure resulting in a loss of confidentiality. Proper management includes tagging, handling, storing and destroying sensitive information. The two areas where organizations often miss the mark are adequately protecting backup media holding sensitive information and sanitizing media or equipment when it is at the end of it's lifecycle.

Describe the three data states. The three data states are at rest, in transit and in use. Data at rest is any data stored on media such as hard drives or external media, data in transit is any data transmitted over a network, encryption methods protect data at rest and in transit. Data in use refers to data in memory and used by an application. Applications should flush memory buffers to remove data after it is no longer needed.

Define DLP. Data loss prevention or DLP solutions detect and block data exfiltration attempts by scanning unencrypted files and looking for keywords and data patterns. Network DLP solutions, including cloud DLP solutions scan files before they leave the network. Endpoint DLP solutions prevent users from copying or printing some files. Compare data destruction methods. Erasing a file doesn't delete it. Clearing media overwrites it with characters or bits. Purging repeats the clearing process multiple times and removes data so that the media can be reused. Degaussing removes data from tapes and magnetic hard drives, but it does not affect optical media or solid state drives. Destruction methods include incineration, shredding, disintegration, pulverizing and melting.

Describe data remnants. Data remnants is the data that remains on media after it should have been removed. Hard disk drives sometimes retain residual magnetic flux that can be read with advanced tools. Advanced tools can also read slack space on a disc, which is unused space and clusters. Erasing data on a disc leaves data remnants. For solid state drives, data remnants can persist due to the wear leveling algorithms they employ making traditional data erasure measures less effective and potentially allowing remnants of data to remain on unaddressed memory cells.

Understand record retention policies. Record retention policies ensure that data is kept in a usable state while it is needed and destroyed when it is no longer needed. Many laws and regulations mandate keeping data for a specific amount of time, but in the absence of formal regulations, organizations specify the retention period within a policy. Audit trail data needs to be kept long enough to reconstruct past incidents, but the organization must identify how far back they want to be able to investigate.

A current trend in many organizations is to reduce legal liabilities by implementing short retention policies with email. Know the difference between end of life and end of support. End of life, EOL is the

date announced by a vendor when the production and sales of a product stop. However, the vendor will still support the product after EOL. End of support identifies the date when a vendor will no longer support a product.

Explain DRM. Digital Rights Management or DRM methods provide copyright protection for copyrighted works. The purpose is to prevent the unauthorized use, modification and distribution of copyrighted work.

Explain CASB, cloud access security broker, CASB is a solution placed logically between users and cloud resources. It can apply internal security controls to cloud resources. The CASB solution can be placed on premises or in the cloud.

Define pseudonymization. Pseudonymization is the process of replacing some data elements with pseudonyms or aliases. It removes private data so that a dataset can be shared. However, the original data remains available in a separate dataset.

Define tokenization. Tokenization replaces data elements with a string of characters or a token. Credit card processors replace credit card data with a token and a third party holds the mapping to the original data and the token.

Define anonymization. Anonymization replaces privacy data with useful but inaccurate data. The dataset can be shared and used for analysis purposes, but anonymization removes individual identities. Anonymization is permanent. Know the responsibilities of data roles. The data owner is the person responsible for classifying, labeling and protecting data.

Data controllers decide what data to process, the purpose of data collection and how to process data. Data processors are third-party entities that process data for an organization at the direction of the data controller. A user accesses data while performing work tasks. The data subject is the person described in personally identifiable information and a custodian has day-to-day responsibilities for protecting and storing data.

Know about security control baselines. Security control baselines provide a listing of controls that an organization can apply as a baseline. Not all baselines apply to all organizations. Organizations apply scoping and tailoring techniques to adapt a baseline to their needs. Those are the study essentials that you'll need to know for Chapter 5, protecting security of assets.

From:
https://trident365.com/ - **三叉戟**

Permanent link:
https://trident365.com/doku.php?id=projects:cissp:chapter5

Last update: **2025/05/18 17:15**