Asset Security

Identify and classify information and assets

- Data classification - indicates the level of confidentiality, integrity, and availability protection that is required
  - Levels: Confidential > Private > Sensitive > Public
- Asset Classification - ^^

Determine and maintain information and asset ownership

Primary information security roles include business or mission owners, data owners, system owners, custodians, and users. Each role has a different set of responsibilities in securing an organization's assets. There should be a plan in place to audit assets atleast every year

Protect privacy

- Data owners - The data/information owner is a manager responsible for ensuring that specific data is protected. Data sensitivity labels and the frequency of data backup is something they decide. They focus on data itself(electronic or paper format). Generally each line of business will have their own data owner. The data owner performs management duties, while custodians perform the hands-on protection of data.
- Data processers - A data controller is someone who controls sensitive data, they own it. A data processor is someone that uses and reads that. An outsourced payroll company is an example of a data processor. Data processors manage payroll data, which is used to determine the amount to pay individual employees, on behalf of a data controller, such as an HR department.
- Data remanence - Data that persists beyond noninvasive means to delete it. Though data remanence is sometimes used specifically to refer to residual data that persists on magnetic storage, remanence concerns go beyond just that of magnetic storage media.
- Collection limitation - There should be limits to the collection of personal data. The subject must consent before this data is collected

Ensure appropriate asset retention

Information stops being useful after a certain amount of time. Sensitive data should have a retention time on it. There may be regulations or legal reasons why an organization may have to keep information for a long time.

Determine data security controls

- Understand data states - data is either at rest or in motion. Different controls apply to them.
- Scoping and tailoring - scoping is deciding which standards will be carried out by organization. Tailoring is customizing that standard towards the organization (like implimenting subplimental controls)
- Standards selection - pick the following: PCI-DSS, OCTAVE, ISO 17799, COBIT, ITIL
- Data protection methods - network encryption, HDD and tape encryption, and transportation protection

Establish information and asset handling requirements

Need to have classification and need to know before accessing information or assets. There should be solid justification for accessing these things.

Home Page
To next domain! - D3 - Security Architecture and Engineering