Identifying and Classifying Assets

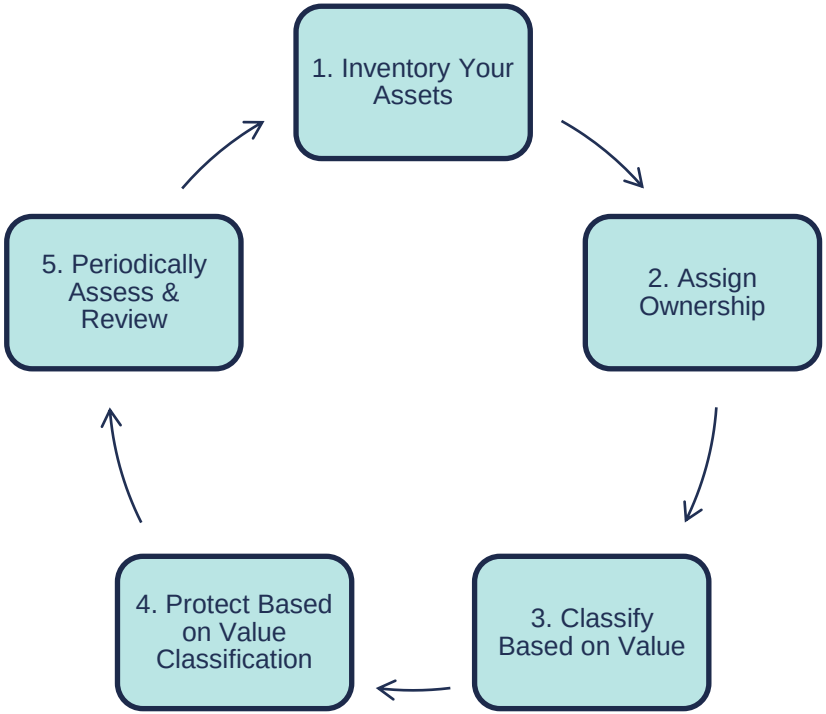
Assets

Anything deemed valuable to a company is considered an asset:

- People
- Information
- Data
- Hardware
- Software
- Processes
- Ideas
- Etc.

You can't effectively protect your organization if you don't know what you have. Therefore, assets should be identified and classified so they can be effectively protected.

Asset Identification & Classification Process



Understanding the Asset Lifecycle

The Asset Lifecycle

1. Identify & Classify	•New assets should be identified and classified.
2. Secure	•Secure assets based on the classified value.
3. Monitor	•Regularly monitor for changes in value and the effectiveness of our security controls.
4. Recovery	•If an asset if adversely impacted, recovery measures should in place.
5. Disposition	•Once the usefulness of an asset been reached and it is to be disposed, there are two primary methods: **archiving** the asset for long-term storage or **defensible destruction**, ensuring there is no data remanence.

Data Retention

Data Retention

- Data retention is the long-term storage of valuable assets, typically driven by:
  - Legal and Regulatory Compliance Requirements
  - Organizational Requirements
- Retaining sensitive information poses a risk to the organization because of data breaches and threats of disclosure.
  - 2017 Equifax Data Breach of 145.5 million U.S. consumers cost the company $1.4 billion
  - 2013 Target Customer Credit/Debit Card Data Breach of 70 million customers cost the company $162 million
- Therefore, sensitive information should only be retained as long as it is useful or required by law.
- Organizations can do so by developing a records retention policy based on legal, regulatory, and organizational requirements.

Understanding Data States

Data States

Data State	Details
Data at Rest	Data that's stored on media of any form (hard drive, USB stick, tape, CD). It's considered at rest because it's not being transmitted over the network or in use. Data at rest is commonly protected by disk and file encryption.
Data in Motion	Data that's currently moving across a network from one device to another. Data in motion is commonly protected by network encryption, such as SSL, TLS, and VPN connections with IPSec encryption.
Data in Use	Data that's being used by a system process, application or user. It's data that's being created, updated, appended, or erased. Data in use is the hardest to protect because it's not encrypted while in use. Proper access control, integrity checks, and auditing measures can help protect data in use.