Chapter 5 – Protecting Security of Assets

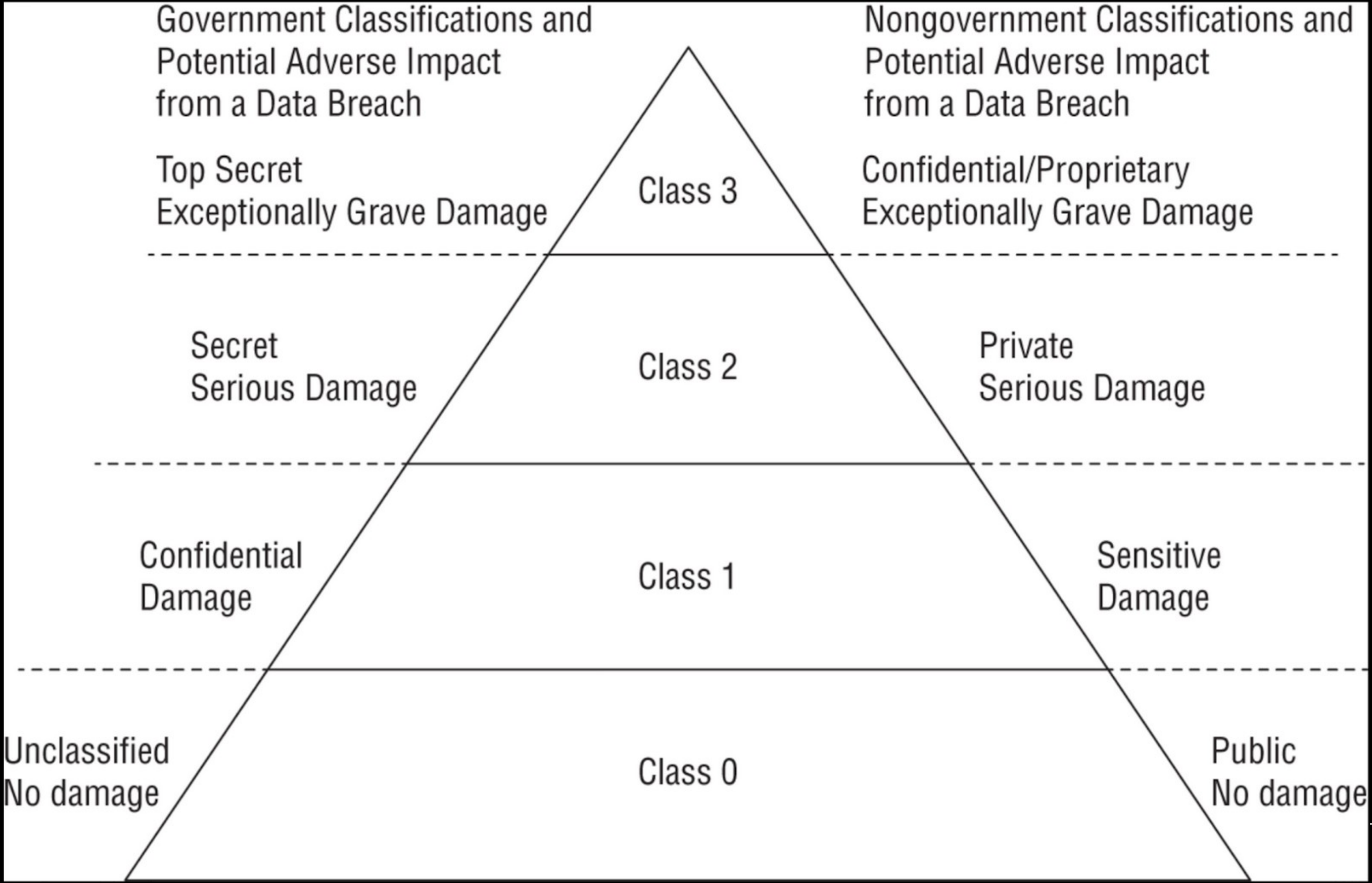
Defining Sensitive Data

- Personally Identifiable Information (PII)
  - NIST SP 800-122
- Protected Health Information (PHI)
  - HIPAA and makes it broad
- Proprietary Data
  - Think about the previous chapter

Defining Data Classifications

- Top Secret
- Secret
- Confidential
- Unclassified

Defining Data Classifications



Government Classifications and Potential Adverse Impact from a Data Breach

Nongovernment Classifications and Potential Adverse Impact from a Data Breach

Top Secret
Exceptionally Grave Damage

Class 3

Confidential/Proprietary
Exceptionally Grave Damage

Secret
Serious Damage

Class 2

Private
Serious Damage

Confidential
Damage

Class 1

Sensitive
Damage

Unclassified
No damage

Class 0

Public
No damage

Defining Asset Classifications

- Asset classification should match the data classifications
- For example: A computer that process top secret data, then the computer is considered a top secret asset

Understanding Data States

- Data at Rest
- Data in Transit
- Data in Use

Compliance Requirements

- Type of data matters
- This relates back to Chapter 4

Determining Data Security Controls

- How would you put controls on the following:
  - Confidential/Proprietary
  - Private
  - Sensitive
  - Public

Information Handling Requirements

- Data Maintenance
- Data Loss Prevention
  - Network DLP, Cloud DLP, Endpoint DLP
- Labeling Sensitive Data and Assets

Handling Sensitive Information/Assets

- Data Collection Limitation
- Data Location
- Storing Sensitive Data

Data Destruction

- Eliminating Data Remanence
- Common Data Destruction Methods
  - Erasing, Purging, Degaussing, Destruction
- Cryptographic Erasure

Appropriate Data & Asset Retention

- Record Retention
- EOL (End of Life)
- EOS (End of Support)

Data Protection Methods

- We talked about DLP
- Digital Rights Management
  - DRM License
  - Persistent Online Authentication
  - Continuous Audit Trail
  - Automatic Expiration

Cloud Access Security Broker (CASB)

- Software between users and cloud based resources
- Authentication and Authorization
- Detects shadow IT

Pseudonyminzation

- Pseudonym for different data sets
- Prevents data from identifying an entity or person
- You can still reverse the data

Tokenization

- Registration
- Usage
- Validation
- Completing a Sale
- Even if someone took a token, it’s extremely difficult to use unless at the time

Anonymization

- If you don’t need personal data, another option is to remove all relevant data
- You can’t detect the original subject or person
- Randomized
- You can’t get the data back

Understanding Data Roles

- Data Owners (CEO, President, Department Head, etc.)
- Data Controllers and Processors (persons collection and use of data)
- Data Custodians (Properly stored/protected)
- Users and Subjects (Personal Information)

Using Security Baselines

- Low-Impact Systems
- Moderate-Impact Systems
- High-Impact Systems
- Privacy Control Baseline

Comparing Tailoring and Scoping

- After selecting a control baseline, we need to fine-tune it
- Tailoring is to modify your baseline
- NIST SP 800-53B
- Standards Selection
  - PCI DSS, GDPR, NIST CSF, CIS, CMMC, etc.