Domain 2 – Asset Security

M. Veeraragaloo
February 2018

Outline

1. Classify information and supporting assets
   a. Sensitivity and Criticality
2. Determine and maintain ownership
   a. Data Owners,
   b. System Owners,
   c. Business / Mission Owners
3. Protect Privacy
   a. Data Owners
   b. Data Processes
   c. Data Remanence
   d. Collection Limitation
4. Ensure appropriate retention (e.g. Media, hardware, personnel)
5. Determine Data Security Controls
   a. Baselines
   b. Scoping and Tailoring
   c. Standards Selection
   d. Cryptography
6. Establish handling requirements
   a. Labels, Storage,
   b. Destruction of Sensitive Information

1. Classifying Information

Classifying Information

1. Organizations often include classification definitions within a security policy. Personnel then label assets appropriately based on the security policy requirements
2. Defining Sensitive Data
    a. Sensitive data is any information that isn't public or unclassified. It can include confidential, proprietary, protected, or any other type of data that an organization needs to protect due to its value to the organization, or to comply with existing laws and regulations

Classifying Information

3. Personal Identifiable Information
   a. Personally identifiable information (PII) is any information that can identify an individual
   b. NIST SP 800-122

   Any information about an individual maintained by an agency, including

      i. any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
      ii. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Classifying Information

4. Protected Health Information
   a. Protected health information (PHI) is any health-related information that can be related to a specific person
   b. HIPAA provides a more formal definition of PHI:

Health information means any information, whether oral or recorded in any form or medium, that—

   i. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
   ii. relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Classifying Information

5. Propriety Data
   a. Proprietary data refers to any data that helps an organization maintain a competitive edge.
   b. It could be software code it developed, technical plans for products, internal processes, intellectual property, or trade secrets.
   c. Although copyrights, patents, and trade secret laws provide a level of protection for proprietary data, this isn't always enough.

Classifying Information

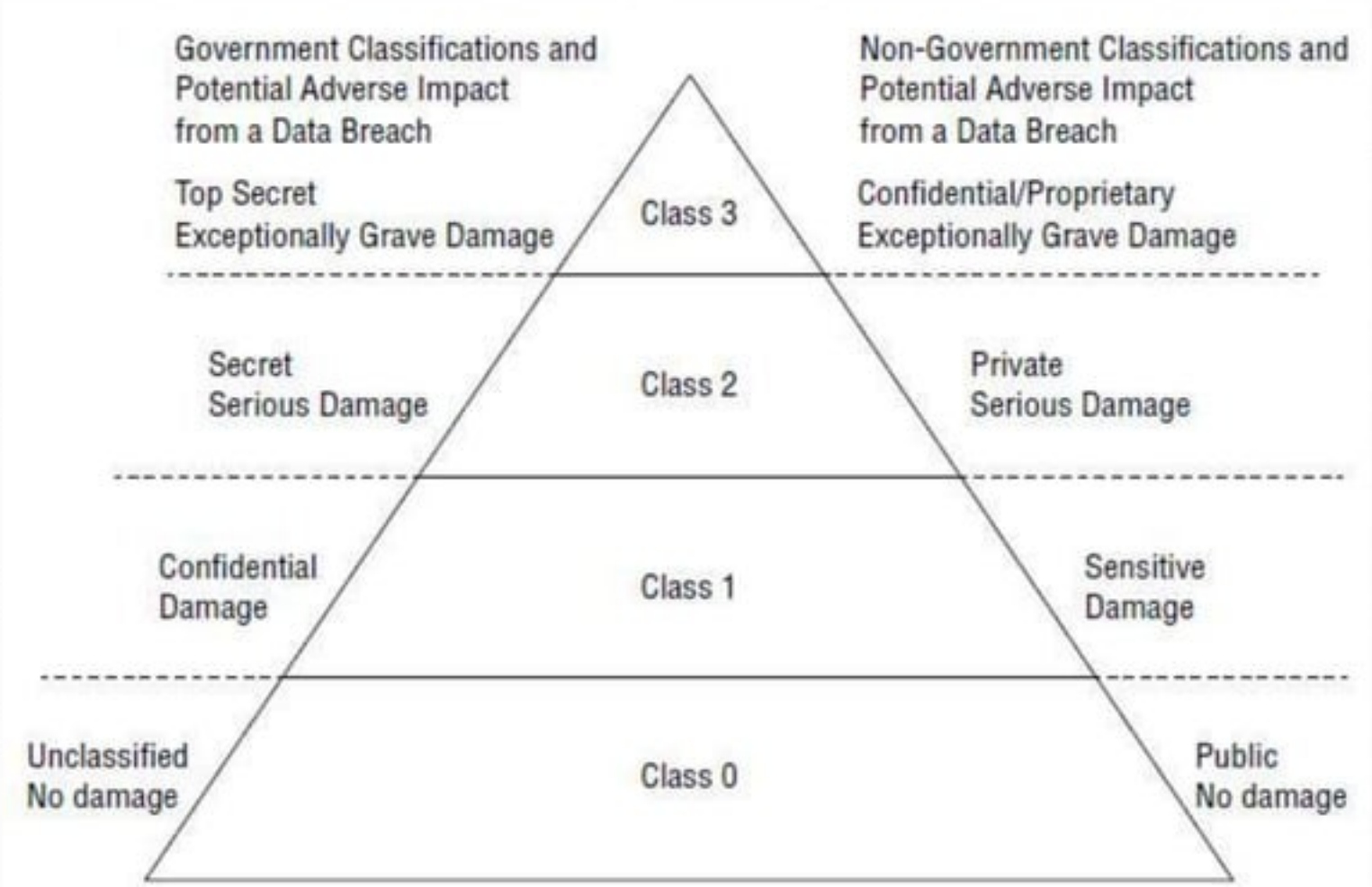
1. Defining Classifications
   a. Organizations typically include data classifications in their security policy, or in a separate data policy.
   b. A data classification identifies the value of the data to the organization and is critical to protect data confidentiality and integrity. The policy identifies classification labels used within the organization.
   c. It also identifies how data owners can determine the proper classification, and personnel should protect data based on its classification

Classifying Information

1. Defining Classifications
   a. Top Secret - The top secret label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe."
   b. Secret - The secret label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."
   c. Confidential - The confidential label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."
   d. Unclassified - Unclassified refers to any data that doesn't meet one of the descriptions for top secret, secret, or confidential data.

Classifying Information

Defining Classifications



Classifying Information

1. Defining Classifications
   e. Confidential or Proprietary - The confidential or propriety label refers to the highest level of classified data. In this context, a data breach would cause exceptionally grave damage to the mission of the organization.
   f. Private - The private label refers to data that should stay private within the organization but doesn't meet the definition of confidential or proprietary data. In this context, a data breach would cause serious damage to the mission of the organization.
   g. Sensitive - Sensitive data is similar to confidential data. In this context, a data breach would cause damage to the mission of the organization.
   h. Public - Public data is similar to unclassified data. It includes information posted in websites, brochures, or any other public source. Although an organization doesn't protect the confidentiality of public data, it does take steps to protect its integrity.

Classifying Information

Defining Data Security Requirements

1. Securing Email

Classification	Security requirements for email
Confidential/Proprietary	Email and attachments must be encrypted with AES 256. Email and attachments remain encrypted except when viewed. Email can only be sent to recipients within the organization. Email can only be opened and viewed by recipients (forwarded emails cannot be opened). Attachments can be opened and viewed, but not saved. Email content cannot be copied and pasted into other documents. Email cannot be printed.
Classification	**Security requirements for email**
Private	Email and attachments must be encrypted with AES 256. Email and attachments remain encrypted except when viewed. Can only be sent to recipients within the organization.
Sensitive	Email and attachments must be encrypted with AES 256.
Public	Email and attachments can be sent in cleartext.

2. Determine and Maintain Ownership

Determine and Maintain Ownership

1. Data Owners
   a. The data owner is the person who has ultimate organizational responsibility for data.
   b. Data owners identify the classification of data and ensure that it is labelled properly.
   c. They also ensure it has adequate security controls based on the classification and the organization's security policy requirements.
   d. NIST SP 800-18 outlines the following responsibilities for the information owner, which can be interpreted the same as the data owner.
      i. Establishes the rules for appropriate use and protection of the subject data/information (rules of behaviour)
      ii. Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides
      iii. Decides who has access to the information system and with what types of privileges or access rights
      iv. Assists in the identification and assessment of the common security controls where the information resides.

Determine and Maintain Ownership

2. System Owners
    a. The system owner is the person who owns the system that processes sensitive data.
    b. NIST SP 800-18 outlines the following responsibilities for the system owner:
        i. Develops a system security plan in coordination with information owners, the system administrator, and functional end users
        ii. Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements
        iii. Ensures that system users and support personnel receive appropriate security training, such as instruction on rules of behaviour (or an AUP)
        iv. Updates the system security plan whenever a significant change occurs
        v. Assists in the identification, implementation, and assessment of the common security controls.

Determine and Maintain Ownership

3. Business / Mission Owners
   a. The business/mission owner role is viewed differently in different organizations.
   b. NIST SP 800-18 refers to the business/mission owner as a program manager or an information system owner.
   c. As such, the responsibilities of the business/mission owner can overlap with the responsibilities of the system owner or be the same role.
   d. Business owners might own processes that use systems managed by other entities.

Determine and Maintain Ownership

4. Data Processes
   a. Generically, a data processor is any system used to process data.
   b. However, in the context of the EU Data Protection law, data processor has a more specific meaning.
   c. The EU Data Protection law defines a data processor as "a natural or legal person which processes personal data solely on behalf of the data controller."
   d. In this context, the data controller is the person or entity that controls processing of the data.

Determine and Maintain Ownership

5. Administrators
   a. A data administrator is responsible for granting appropriate access to personnel.
   b. They don't necessarily have full administrator rights and privileges, but they do have the ability to assign permissions.
   c. Administrators assign permissions based on the principles of least privilege and the need to know, granting users access to only what they need for their job.
   d. Administrators typically assign permissions using a role-based access control model.
   e. In other words, they add user accounts to groups and then grant permissions to the groups.

Determine and Maintain Ownership

6. Custodians
   a. Data owners often delegate day-to-day tasks to a custodian.
   b. A custodian helps protect the integrity and security of data by ensuring it is properly stored and protected.
   c. For example, custodians would ensure the data is backed up in accordance with a backup policy.
   d. If administrators have configured auditing on the data, custodians would also maintain these logs.

Determine and Maintain Ownership

7. Users
   a. A user is any person who accesses data via a computing system to accomplish work tasks.
   b. Users have access to only the data they need to perform their work tasks.
   c. You can also think of users as employees or end users.

3. Protect Privacy

Protect Privacy

1. Organizations have an obligation to protect data that they collect and maintain.
2. Many laws require organizations to disclose what data they collect, why they collect it, and how they plan to use the information.
3. Additionally, these laws prohibit organizations from using the information in ways that are outside the scope of what they intend to use it for.
4. When protecting privacy, an organization will typically use several different security controls.
5. Selecting the proper security controls can be a daunting task, especially for new organizations.
6. However, using security baselines and identifying relevant standards makes the task a little easier.

Protect Privacy

Using Security Baselines

1. Baselines provide a starting point and ensure a minimum security standard.
2. As an introduction, administrators configure a single system with desired settings, capture it as an image, and then deploy the image to other systems.
3. This ensures all of the systems are deployed in a similar secure state.
4. After deploying systems in a secure state, auditing processes periodically check the systems to ensure they remain in a secure state.
5. NIST SP 800-53 discusses security control baselines as a list of security controls.
6. It stresses that a single set of security controls does not apply to all situations, but any organization can select a set of baseline security controls and tailor it to its needs.

Protect Privacy

Scoping and Tailoring

1. Scoping refers to reviewing baseline security controls and selecting only those controls that apply to the IT system you're trying to protect.
2. Tailoring refers to modifying the list of security controls within a baseline so that they align with the mission of the organization.

Protect Privacy

Selecting Standards

1. When selecting security controls within a baseline, or otherwise, organizations need to ensure that the controls comply with certain external security standards.
2. With this in mind, organizations need to identify the standards that apply, and ensure the security controls they select comply with these standards.

4. Ensure Appropriate Retention

Ensure Appropriate Retention

Retaining Assets

a. Retention requirements apply to data or records, media holding sensitive data, systems that process sensitive data, and personnel who have access to sensitive data.
b. Record retention and media retention is the most important element of asset retention.
c. Record retention involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed.
d. An organization's security policy or data policy typically identifies retention timeframes.
e. Some laws and regulations dictate the length of time that an organization should retain data, such as three years, seven years, or even indefinitely.

5. Determine Data Security Controls

Determine Data Security Controls

Understanding Data States

1. It's important to protect data while it is at rest, in motion, and in use.
2. Data at rest is any data stored on media such as system hard drives, external USB drives, storage area networks (SANs), and backup tapes.
3. Data in transit (sometimes called data in motion) is any data transmitted over a network. This includes data transmitted over an internal network using wired or wireless methods and data transmitted over public networks such as the Internet.
4. Data in use refers to data in temporary storage buffers while an application is using it.

Determine Data Security Controls

Protecting Confidentiality with Cryptography

1. **Protecting Data with Symmetric Encryption**
    1. Symmetric encryption uses the same key to encrypt and decrypt data.
    2. Symmetric algorithms don't use the same key for different data.
    3. Advanced Encryption Standard - The Advanced Encryption Standard (AES) is one of the most popular symmetric encryption algorithms.
        i. AES supports key sizes of 128 bits, 192 bits, and 256 bits
    4. Triple DES - Developer's created Triple DES (or 3DES) as a possible replacement for DES.
        i. The first implementation used 56-bit keys but newer implementations use 112-bit or 168-bit keys.
        ii. Larger keys provide a higher level of security.
    5. Blowfish - Security expert Bruce Schneier developed Blowfish as a possible alternative to DES.
        i. It can use key sizes of 32 bits to 448 bits and is a strong encryption protocol.
        ii. Linux systems use bcrypt to encrypt passwords, and bcrypt is based on Blowfi sh.
        iii. Bcrypt adds 128 additional bits as a salt to protect against rainbow table attacks.

Determine Data Security Controls

Protecting Confidentiality with Cryptography

2. Protecting Data with Transport Encryption

1. Transport encryption methods encrypt data before it is transmitted, providing protection of data in transit.
2. Almost all HTTPS transmissions use Transport Layer Security (TLS) as the underlying encryption protocol. Secure Sockets Layer (SSL) was the precursor to TLS.
3. In 2014, Google discovered that SSL is susceptible to the POODLE attack (Padding Oracle On Downgraded Legacy Encryption)
4. Organizations often enable remote access solutions such as virtual private networks (VPNs).
5. VPNs allow employees to access the organization's internal network from their home or while travelling.
6. VPN traffic goes over a public network, such as the Internet, so encryption is important. VPNs use encryption protocols such as TLS and Internet Protocol security (IPsec).
7. IPsec is often combined with Layer 2 Tunneling Protocol (L2TP) for VPNs.
8. L2TP transmits data in cleartext, but L2TP/IPsec encrypts data and sends it over the Internet using Tunnel mode to protect it while in transit.
9. IPsec includes an Authentication Header (AH), which provides authentication and integrity, and Encapsulating Security Payload (ESP) to provide confidentiality.

6. Establish Handling Requirements

Establish Handling Requirements

Managing Sensitive Data

a. A key goal of managing sensitive data is to prevent data breaches.
b. A data breach is any event in which an unauthorized entity is able to view or access sensitive data.

1. Marking Sensitive Data
   a. Marking (often called labelling) sensitive information ensures that users can easily identify the classification level of any data.
   b. The most important information that a mark or a label provides is the classification of the data.
   c. Marking includes both physical and electronic marking and labels.
   d. Physical labels indicate the security classification for the data stored on media or processed on a system.
   e. Physical labels remain on the system or media throughout its lifetime.
   f. Marking also includes using digital marks or labels. A simple method is to include the classification as a header and/or footer in a document, or embed it as a watermark.

Establish Handling Requirements

Managing Sensitive Data

2. Handling Sensitive Data
   a. Handling refers to the secure transportation of media through its lifetime.
   b. Policies and procedures need to be in place to ensure that people understand how to handle sensitive data. This starts by ensuring systems and media are labelled appropriately.
3. Storing Sensitive Data
   a. Sensitive data should be stored in such a way that it is protected against any type of loss. The obvious protection is encryption.

Establish Handling Requirements

Managing Sensitive Data

4. Destroying Sensitive Data
   a. An organization's security policy or data policy should define the acceptable methods of destroying data based on the data's classification.
   b. Data remanence is the data that remains on a hard drive as residual magnetic fl ux. Using system tools to delete data generally leaves much of the data remaining on the media, and widely available tools can easily undelete it.
   c. One way to remove data remanence is with a degausser.
   d. A degausser generates a heavy magnetic field, which realigns the magnetic fields in magnetic media such as traditional hard drives, magnetic tape, and floppy disk drives.
   e. However, they are only effective on magnetic media.

Establish Handling Requirements

Managing Sensitive Data

4. Destroying Sensitive Data

The following list includes some of the common terms associated with destroying data:

a. Erasing - Erasing media is simply performing a delete operation against a file, a selection of files, or the entire media. In most cases, the deletion or removal process removes only the directory or catalogue link to the data.

b. Clearing - Clearing, or overwriting , is a process of preparing media for reuse and assuring that the cleared data cannot be recovered using traditional recovery tools. When media is cleared, unclassified data is written over all addressable locations on the media.

c. Purging - 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. A purging process will repeat the clearing process multiple times and may combine it with another method such as degaussing to completely remove the data.

Establish Handling Requirements

Managing Sensitive Data

4. Destroying Sensitive Data

The following list includes some of the common terms associated with destroying data:

d. Declassification - Declassification involves any process that purges media or a system in preparation for reuse in an unclassified environment. Purging can be used to prepare media for declassification, but often the efforts required to securely declassify media are significantly greater than the cost of new media for a less secure environment.

e. Sanitization - Sanitization is a combination of processes that removes data from a system or from media. It ensures that data cannot be recovered by any means. When a computer is disposed of, sanitization includes ensuring that all non-volatile memory has been removed or destroyed, the system doesn't have CD/DVDs in any drive, and internal drives (hard drives and SSDs) have been purged, removed, and/or destroyed. Sanitization can refer to the destruction of media or using a trusted method to purge classified data from the media without destroying it.

Establish Handling Requirements

Managing Sensitive Data

4. Destroying Sensitive Data

The following list includes some of the common terms associated with destroying data:

f. Degaussing A degausser creates a strong magnetic field that erases data on some media in a process called degaussing. Technicians commonly use degaussing methods to remove data from magnetic tapes with the goal of returning the tape to its original state. It is possible to degauss hard disks, but we don't recommend it. Degaussing does not affect optical CDs, DVDs, or SSDs.

g. Destruction - Destruction is the final stage in the life cycle of media and is the most secure method of sanitizing media. When destroying media it's important to ensure that the media cannot be reused or repaired and that data cannot be extracted from the destroyed media. Methods of destruction include incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals.

Conclusion

References

- CISSP Study Guide – 7th Edition