2022 | 2023

Network and Information Systems Security

Asset Security

Carlos Serrão

carlos.serrao@iscte-iul.pt

iscte INSTITUTO UNIVERSITÁRIO DE LISBOA

Summary

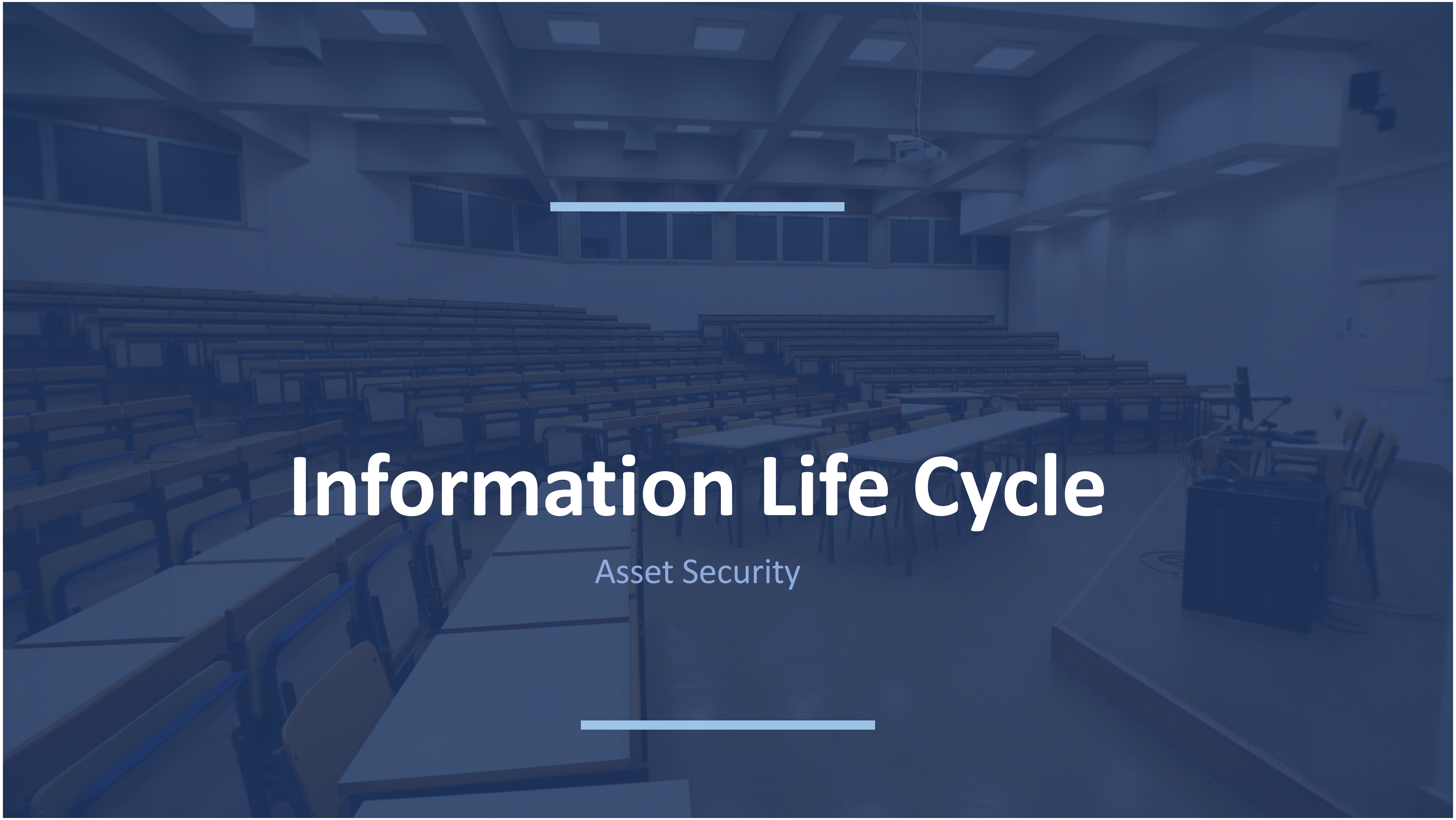
Topics to discuss in this section

- Information Life Cycle
- Roles and Responsibilities
- Information and Asset Classification
- Data Retention

Asset

Definition

- An **information asset** is any **data**, **device** or **other component** of the environment that **supports information** or the **activities** of an information system
  - The **value** of the asset is given by the owners of the asset, authorized and unauthorized users
    - It may include the cost of the responsibility or compromise of the same
  - The **cost of the asset** is the amount it costs to acquire, develop, maintain or replace

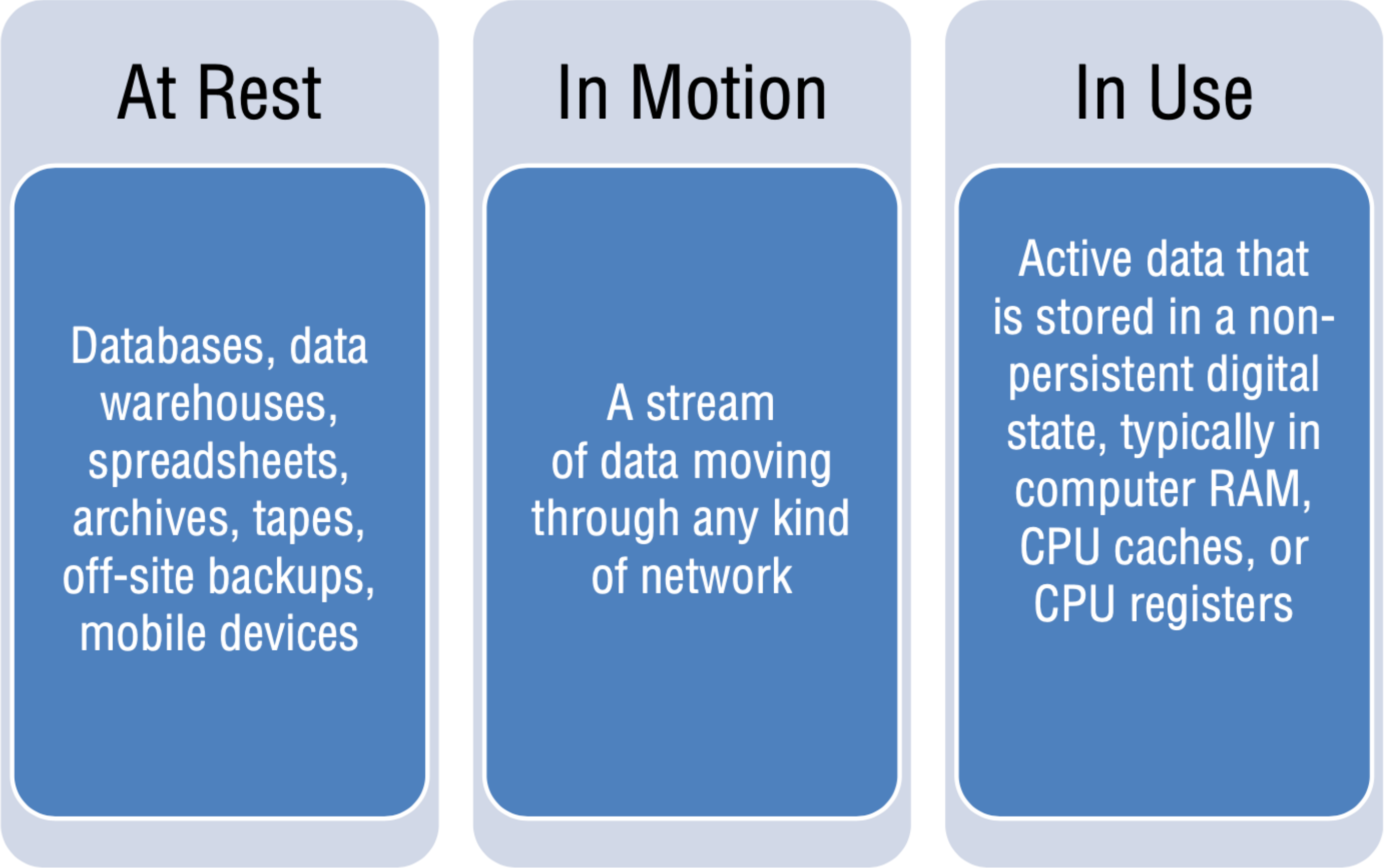


Information Life Cycle

Asset Security

Data States

Information Life Cycle



At Rest

Databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices

In Motion

A stream of data moving through any kind of network

In Use

Active data that is stored in a non-persistent digital state, typically in computer RAM, CPU caches, or CPU registers

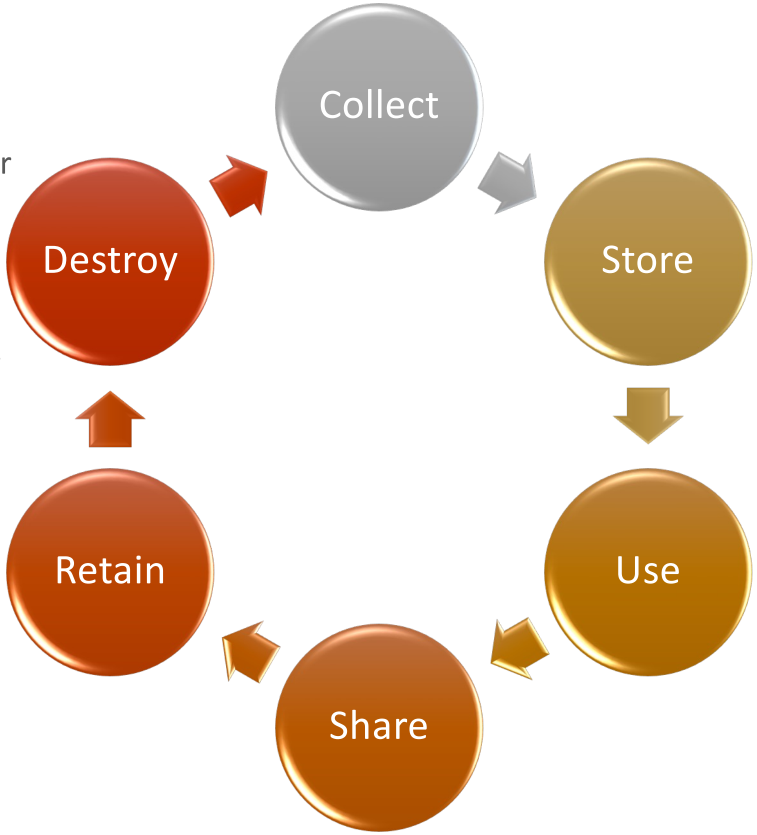
Source: The Official (ISC)2 CISSP CBK Reference

Information lifecycle

Different stages of the Information Lifecycle

⇢**Information lifecycle**:

1. Collect: Data is generated or aggregated.
2. Store: Data is saved into a storage system or repository.
3. Use: Data is processed and/or analyzed, by users or systems, for its intended purposes.
4. Share: Data is shared with authorized external users and systems.
5. Retain: Data is kept (e.g., archived) for a predefined period of time.
6. Destroy: Data is deleted and permanently removed from storage, making it inaccessible and unusable.



The **CIA** of valuable (sensitive) information assets should be properly protected during the **asset lifecycle**.

Source: The Official (ISC)2 CISSP CBK Reference

Sensitive Data

Information lifecycle

- **Losses can occur if the CIA is compromised**
- Intellectual Property (IP)
  - Business secrets, patents, copyrights, trademarks
  - R&D, business or marketing plans, financial data, customer lists
- Personally Identifiable Information (PII)
  - Customers, employees, suppliers (GDPR, NIST SP 800-122)
- Personal health information (PHI)
  - PHI – Protected Health Information (HIPAA)
- Payment card holders data

Personally identifiable information (PII) is any information that can identify an individual.

Any information about an individual maintained by an agency, including
(1) 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
(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

NIST SP 800-122

Storage of valuable information assets

Information lifecycle

- **Where are valuable information assets stored?**
  - ***In-house***:
    - Servers, workstations, SAN, laptops, BYOD, smartphones, removable devices, email, printed papers
  - ***Not in-house***:
    - Cloud, third parties, in service providers, laptops, BYOD, smartphones, removable devices, email, printed papers

Access control

Information lifecycle

- **What allows/controls access?**
  - **Technical**, **Administrative** and **Physical** controls
    - Firewalls, routers, permissions/ACLs, DLP, cryptography, policies, contracts, locks, barriers
  - **Isolate/segment** the **most sensitive** data from **less sensitive data** and **deauthorize** access to data

CIA data threats

Information lifecycle

- Confidentiality
  - System and user accounts compromise
  - Loss or theft of laptop, removable media, printed content
  - *Eavesdropping*, *shoulder surfing*, *dumpster diving*
  - *Sniffer*
- Integrity
  - Errors and omissions, fraud, man-in-the-middle
- Availability
  - Hard-Drive crash
  - Servers failure
  - Network failures
  - Corruption
  - DoS, DDoS

Roles and Responsibilities

Asset Security

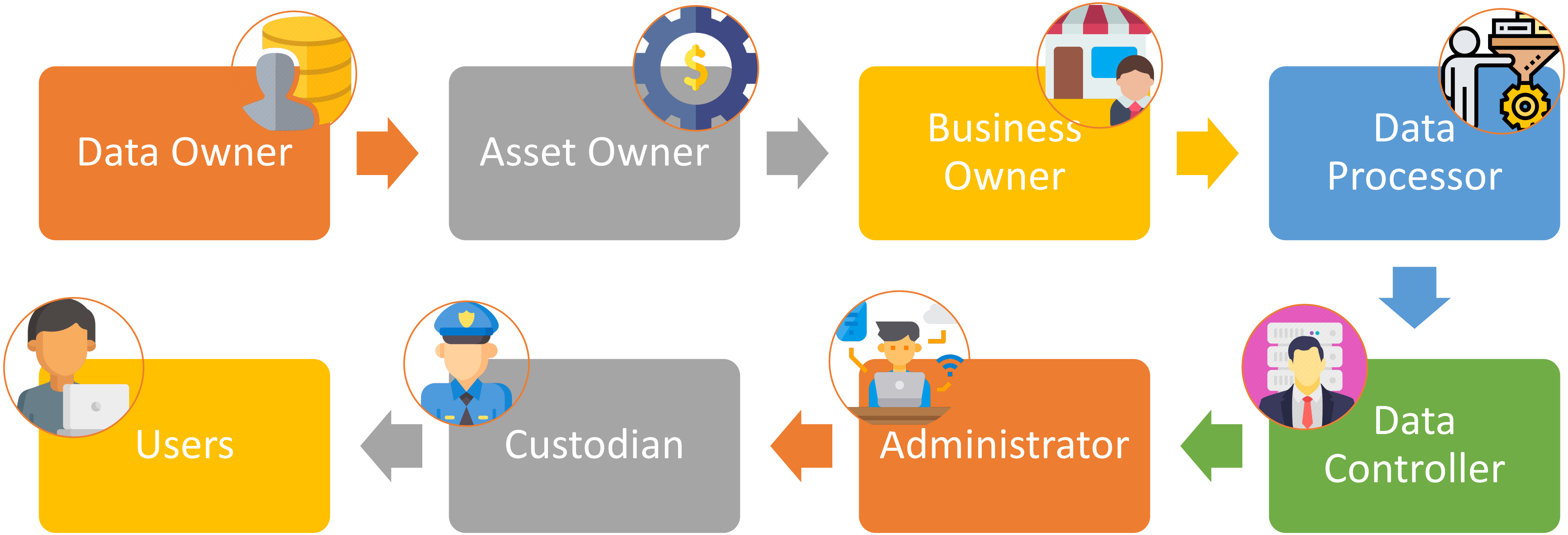
Data Retention

Data retention

- **Data retention** should be **understood** by the **organization**
- Intellectual property rights can be held at various levels
- The **legal retention of data** should be **made clear to avoid risks of improper management** that **causes bad use**, **negligence** or **loss**.

Roles and Responsibilities

Roles and Responsibilities


Data Owner

Asset Owner

Business Owner

Data Processor

Data Controller

Administrator

Custodian

Users

Data Owner

Roles and Responsibilities

- **Establishes** the **rules** for the **proper use** and **protection** of **data/information**
- **Provides input** to the **owners of the organization's information systems** on the **security requirements and security control**s of the **information systems** in which the **information resides**.
- **Decides who has access** to the **information system** and **what types of privileges** or **access rights**.
- **Assists** in **identifying and evaluating the security checks** of the system **in which the information resides**.

Asset Owner

Roles and Responsibilities

Develops a **system security plan** in coordination with **information owners**, **system administrator**, and **end users**.

Maintains the **system security plan** and **ensures that the system is installed** and **operated** as set out in the **agreed requirements**.

Ensures that **system users** and **support personnel receive the appropriate security training**, including acceptable user policies.

Updates the **system security plan** whenever a significant change occurs.

Helps in **identifying**, **implementing**, and **evaluating security controls**.

Business Owner

Roles and Responsibilities

- Must guide the **Security Program**
- Defines **risk tolerance**
- **Depends** on the **security professional** for the **vision** and **justify the costs** of the **recommendations** to **manage the risk**
- **Approves** specific **countermeasures** that **produce** the "**security posture**" **desired** for the organization

Data Processor

Roles and Responsibilities

A “**natural**” or **legal person, public authority**, **agency**, or **any other entity** that **processes personal** data for the **Data Controller**.

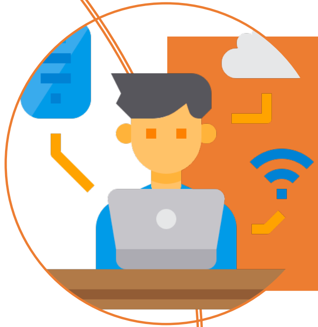
Data Controller

Roles and Responsibilities

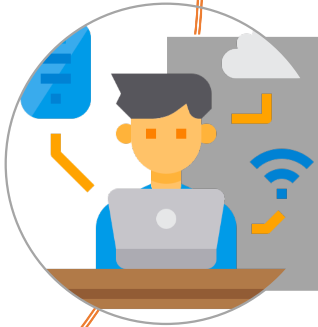
Person or **entity** that **controls** the **data processing.**

Administrator

Roles and Responsibilities



A **Data Administrator** is **responsible** for **assigning proper access** to personnel.



Usually **use RBAC policies.**

Custodian

Roles and Responsibilities

The **Data Owner delegates daily tasks** to a **Custodian**.

Custodian helps **protect** the **integrity** and **security** of data by **ensuring that it is stored conveniently** and **protected**.

In **practice**, **personnel** in the **IT department** or **security administrators** assume the **role of Custodian**.

It can be the **same administrators** who **assign permissions to the data**.

Users

Roles and Responsibilities

A **person** who **accesses data** through a **computer system** to **fulfill their work tasks.**

Users **have access only** to **the data** they **need to perform** their **work tasks**.

Users are **employees** (end-users)

Roles

Roles and Responsibilities

- Data Owner
  - Person with the **utmost responsibility** for the **organization's data**
  - Often a **manager of a division of the organization** (CEO, President, Head of department)
  - **Responsible** for **all aspects** of **its division** (in particular for profits and losses)
- Asset/System Owner
  - Person **holding the asset** or **system that processes sensitive data**
  - **Privileged technician** **responsible** for **implementing security controls**, following the **security policies**
    - Hardware and software maintenance and upgrade
    - System and applications configuration
    - Support systems - power, HVAC, etc.
- Data Processors
  - **Any system** that **processes data**
  - In **GDPR**, "*a natural or legal **person**, public **authority**, **agency**, or other **body**, which processes personal data solely on behalf of the data controller.*"
  - In this context a "***Data Controller***", is a person or entity that **controls the data processing**
- Administrators
  - A data administrator is responsible for **assigning appropriate access** to third parties.
- Custodians
  - **Data owners** delegate **daily tasks** to a custodian.
  - Help protect data integrity and security by ensuring that data is properly stored and protected.
- User
  - Has the **need to access information assets**, IT resources
    - Introduces and processes data, produces reports, takes action on results, helps make better business decisions, improves productivity.

Third-Party Roles

Roles and Responsibilities

- Service providers
  - **External entities** that **store**, **process**, or **transmit** **sensitive data**
    - Cloud services: IaaS, PaaS, SaaS, storage, security
- All **third parties** **dealing with your data** should be **prudently** **required to remain fully in compliance** with the **organization's policy** and **applicable laws** and **regulations**
  - IPR, Privacy (GDPR), HIPAA, SOX, GLBA, PCI-DSS, etc.

Data and Asset Classification

Asset Security

Data and Asset Classification

Introduction

- The **objective** of a **classification system** is to **ensure that information is marked** in such a way that **only those who have a certain level of access** **can access it**
  - Classification is primarily concerned with access
- Each **classification level** must have its **own requirements** for **handling** and **destroying** the asset

Data Classification Program

Data and Asset Classification

- Must be **included/defined** as a **project** within the **several organization policies**
- **Mandatory** for **each data element** (file, database, email)
- **Data owner** is **responsible** for this **data classification program**
- **Data classification tasks** are usually **delegated to subordinate managers** and **users**
- **System/data owners** are **responsible** for **implementing** and **maintaining protections**
- **Managers** and **users** must **know**, **understand** and **be aligned** with **data classification policies** and **protection requirements**
- **Monitoring** and **breach detection** is mandatory
- Managers are **enforcers**
  - Must execute consistently

Data Classification Program

Data and Asset Classification

- Must be perfectly **aligned with applicable laws** and **regulations**
  - HIPAA, SOX, GLBA, PCI, privacy (PII) and others
- Defines **exceptions, whenever necessary**
  - By business necessity
  - Court order
  - Other
- **Rating level must be reviewed annually**
  - **Asset value changes over time**
  - Too low = asset under-protected, increased risk
  - Too high = waste of security budget
- Define the **declassification criteria**
  - When there is no problem **declassifying** (**no longer of value**)
  - **Public disclosure** or **secure destruction**

Primary Types of Data Classification

Data and Asset Classification

- **Context-based**: Derived from **metadata** like **ownership**, **location**, or **other values** that **can indirectly indicate sensitivity** or **criticality**.
- **Content-based**: Derived by **inspecting the contents of files** and directly **identifying sensitive data**, rather than inferring it from metadata.
- **User-based**: Involves **manual assignment of data classification** and is **based on users' understanding** of **the data** and your **organization's classification scheme**.

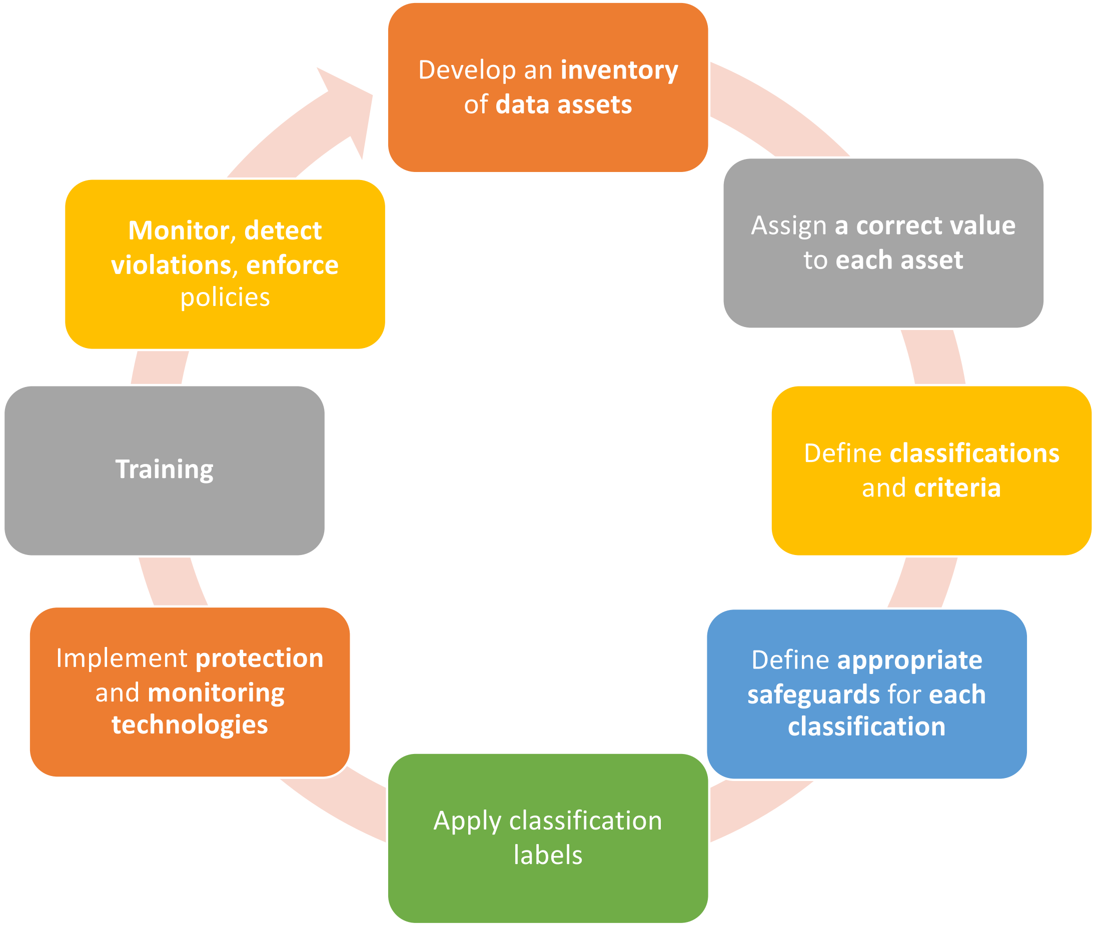
Asset Classification Benefits

- Make an accurate asset inventory
- Gain insight into the environment
- Optimize change, vulnerability, and patch management programs
- Determine the best maintenance windows
- Improve security controls and segmentation
- Tailor protection of sensitive data
- Identify rogue assets
- Understand potential risks posed by vulnerabilities
- Identify proprietary assets and intellectual property
- Forecast costs of protection
- Compliance / Regulatory controls

Source: The Official (ISC)2 CISSP CBK Reference

Data Classification Process

Data Classification Program



Develop an **inventory** of **data assets**

Assign **a correct value** to **each asset**

Define **classifications** and **criteria**

Define **appropriate safeguards** for **each classification**

Apply classification labels

Implement **protection** and **monitoring technologies**

Training

Monitor, detect violations, enforce policies

[1] Develop an inventory of data assets

Data Classification Process

- Files, databases, emails, printed reports, removable devices
- Know **where they are**, who **owns them**, **who the users are**
- **Data in transit**
  - On the company's wired network, over wi-fi, email, WAN connections, Internet
- **Data at rest**
  - On servers, on workstations, laptops, personal devices
  - On HDDs, backup tapes, optical disks
  - On screen
  - Printed data
  - Multiple copies, locations

[2] Assign a correct value to each asset

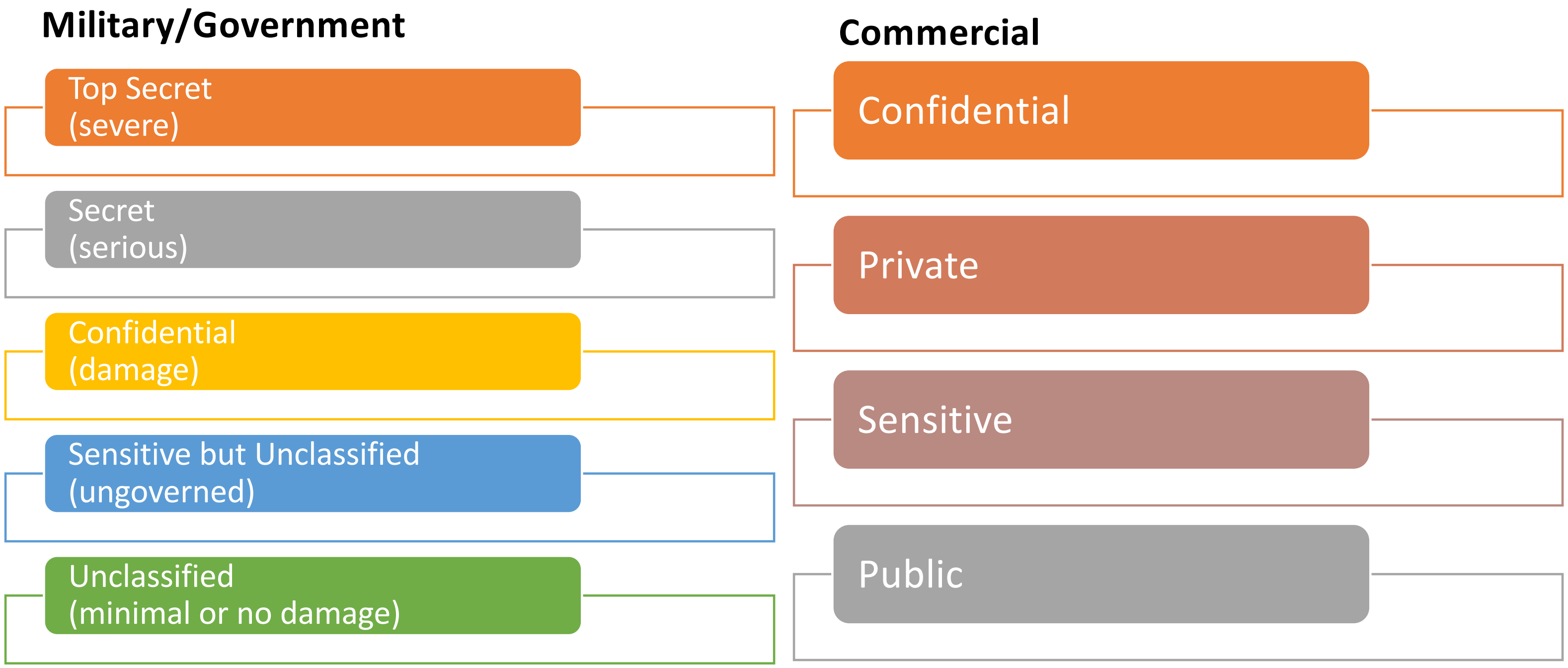
Data Classification Process

- **Losses** if the **CIA** is **compromised**
- How much would **competitors pay for the information**?
- **Penalties**/**liability**/**litigation** if **compromised**
- Potential for **fraud**
- **Losses** if **poor business decisions are made** because of **incorrect or missing data**

[3] Define classifications and criteria

Data Classification Process

- 4 or 5 **levels of classification** are **typical**
- Criteria **should not be ambiguous**



Military/Government

- Top Secret (severe)
- Secret (serious)
- Confidential (damage)
- Sensitive but Unclassified (ungoverned)
- Unclassified (minimal or no damage)

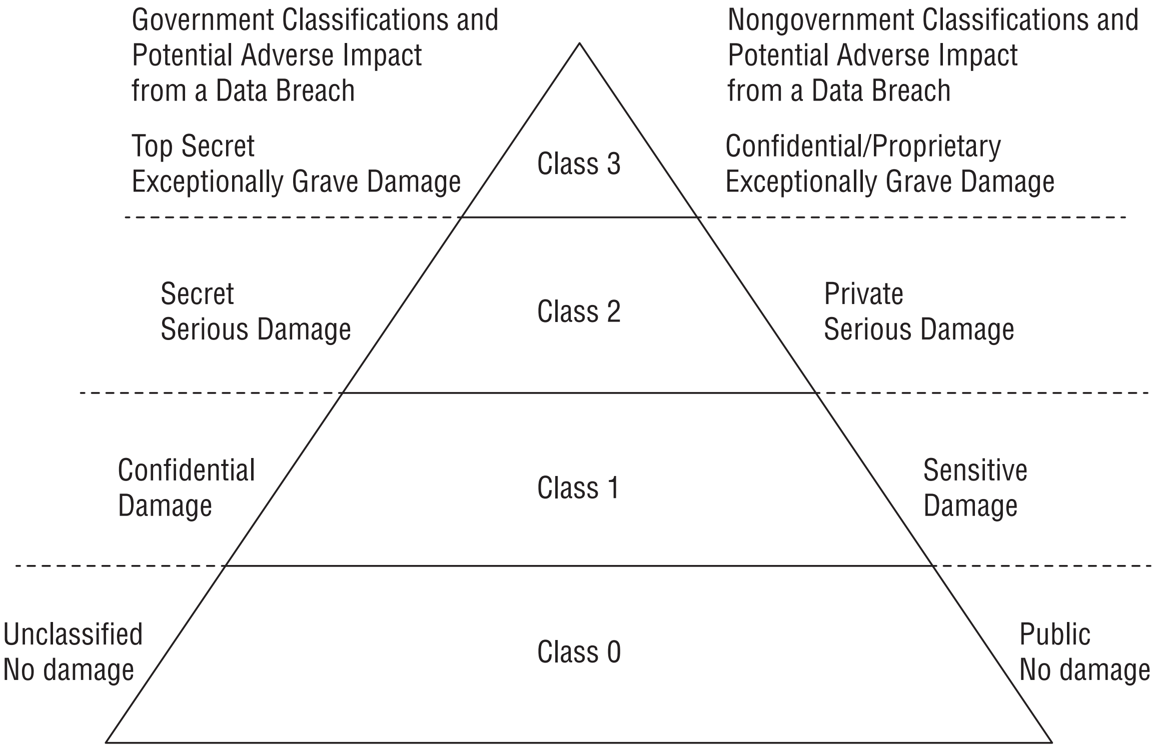
Commercial

- Confidential
- Private
- Sensitive
- Public

[3] Define classifications and criteria

Data Classification Process

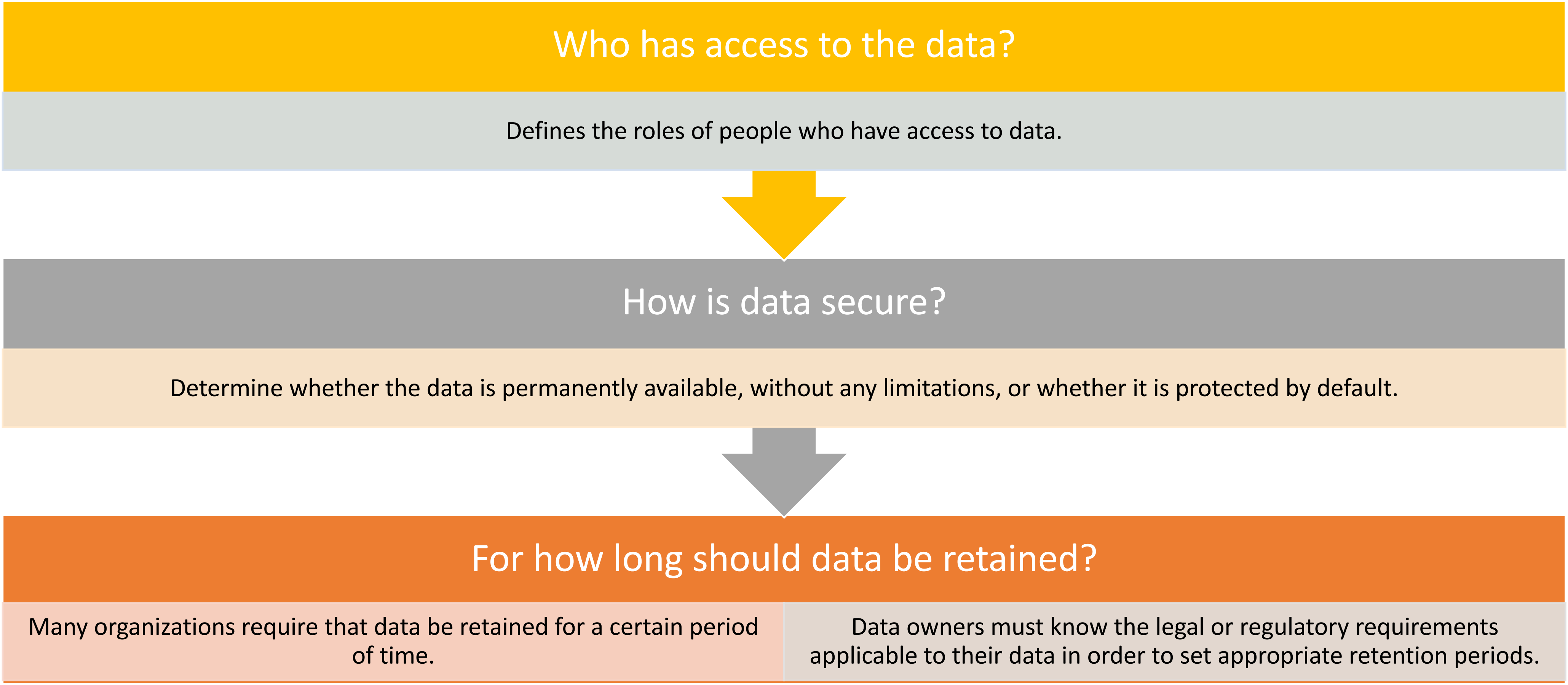
Source: Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.



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

[3] Define classifications and criteria

Data Classification Process



Who has access to the data?

Defines the roles of people who have access to data.

How is data secure?

Determine whether the data is permanently available, without any limitations, or whether it is protected by default.

For how long should data be retained?

Many organizations require that data be retained for a certain period of time.

Data owners must know the legal or regulatory requirements applicable to their data in order to set appropriate retention periods.

[4] Define appropriate safeguards for each classification

Data Classification Process

- Accessible only to certain individuals or job functions
- "Need to know"/"least privilege" (always)
- Multi-factor/mutual authentication requirements
- Encryption of data at rest or in transit
- Do not distribute externally without NDA
- Data redundancy, co-location (availability)
- Monitoring, auditing, breach detection/protection

[5] Apply classification labels

Data Classification Process

- **Align asset value** with **rating ranges**
- **Labels** on **removable devices**
  - The label represents the highest rating level on the device
  - Redesign backups to be aligned with the classification
- **Labels** in headers, footer, watermarks, metadata, etc.

[6] Implement protection and monitoring technologies

Data Classification Process

- Strong Authentication Technologies
- Permissions, ACLs
- TPM, full disk encryption, encrypted storage, file encryption, VPN, SSL/TLS, SSH
- Data Loss Prevention (DLP)
- Message hashes, hash values
- Backups, mirrors, shadowing, co-location

[6] Implement protection and monitoring technologies

Data Classification Process

Classification	Email Security Requirements
Confidential	Email and attachments must be encrypted using AES 256. Email and attachments must remain encrypted except when viewed. They can only be sent to others who belong to the organization. Email can only be opened and viewed by the recipients of the email. Attachments can be opened and viewed, but not saved. The contents of the email cannot be copied and pasted into other documents. Email cannot be printed.
Private	Email and attachments must be encrypted using AES 256.Email and attachments must remain encrypted except when they are viewed.They can only be sent to other elements that belong to the organization.
Sensitive	Email and attachments must be encrypted using AES 256.
Public	Email and attachments can be sent in clear.

[7] Training

Data Classification Process

- **All users must know** and **follow data classification policies** - **including third parties**
- Users must know how to use protection technologies
- Compliance is not optional
- Penalties for violations
- Annual training, upon joining the organization, or when violations occur

[8] Monitor, detect violations, enforce policies

Data Classification Process

- Security team uses technologies to monitor and detect
- First line managers must detect violations and enforce policies
- Enforcement must be constant
- Too much risk to the organization if users do not follow policies - termination, civil or criminal lawsuits

Data Retention

Asset Security

Data Retention

Introduction

- Data **must be kept securely** (CIA) as long **as it is relevant to business useful time**, as **long as it has value to the business**
- Some **laws** and **regulations** specify **specific retention periods beyond** this "**business useful time**", sometimes several years, and **require specific protection** and **availability** mechanisms during the **retention period**
- Retention periods **vary widely**
  - Typically 2 to 10 years
  - Some federal regulations (US) require retention periods of 75 years

Security professionals have to stay aware of the various local, national, and international developments that can impact record retention requirements. An example is the enactment and enforcement of the **EU GDPR's Article 17, "The Right to Erasure,"** commonly called the ***right to be forgotten***. This causes organizations to evaluate previous record retention requirements against the right to be forgotten considerations introduced by Article 17.

This provision gives explicit rights to individuals to have their records erased without undue delay. There is an **exception** for **instances** where the business or data controller **must keep the data for the purposes for which it was collected** (i.e., the original business requirement). In this instance, a business requirement can create an exception to regulatory guidance.

Records Retention Best Practices

Data Retention

- Maintain records according to the organization’s record retention schedule.
- Conduct regular evaluations of the system.
- Conduct a review of the actual record retention schedule every year to make sure the schedule is relevant to business requirements and regulatory requirements.
- Label electronically maintained records.
- Create backup electronic file copies.
- Retain paper copies of records that cannot be accurately or completely transferred to the electronic recordkeeping system.
- Do not keep records longer than is necessary to accomplish the original purpose for which the information was collected.
- Make sure records have valid dates of origin. Movement and use of records can change electronic file dates, but not the date that determines the retention period.
- A reasonable attempt should be made to remove unnecessary electronic records, per the retention schedule, in all identified electronic repositories.
- Maintain information-handling controls over the full lifecycle of information, in some cases extending beyond the disposal of the records.
- Ensure that records remain persistently accessible for the length of the time they are retained according to the frequency with which they are retrieved.
- Deduplicate records to avoid unnecessary storage of multiple copies that increase risk and storage costs.
- Remember to classify and retain emails that are official records. Create an email retention schedule as a subset of the records retention schedule.
- Ensure that records remain accessible for the required retention period by periodically converting and migrating records from media sources, because digital media can degrade or become obsolete over time.
- Securely delete data in accordance with written retention periods and information security and retention policies.

Handling Data and Devices

Data Retention

- All users must **handle data** and **removable devices** according to the **data classification requirements defined** by the **organization**
  - Backup tapes
  - Optical disks - CD, DVD
  - External disks
  - Flash memory - USB sticks, SD, etc.
  - Printed materials

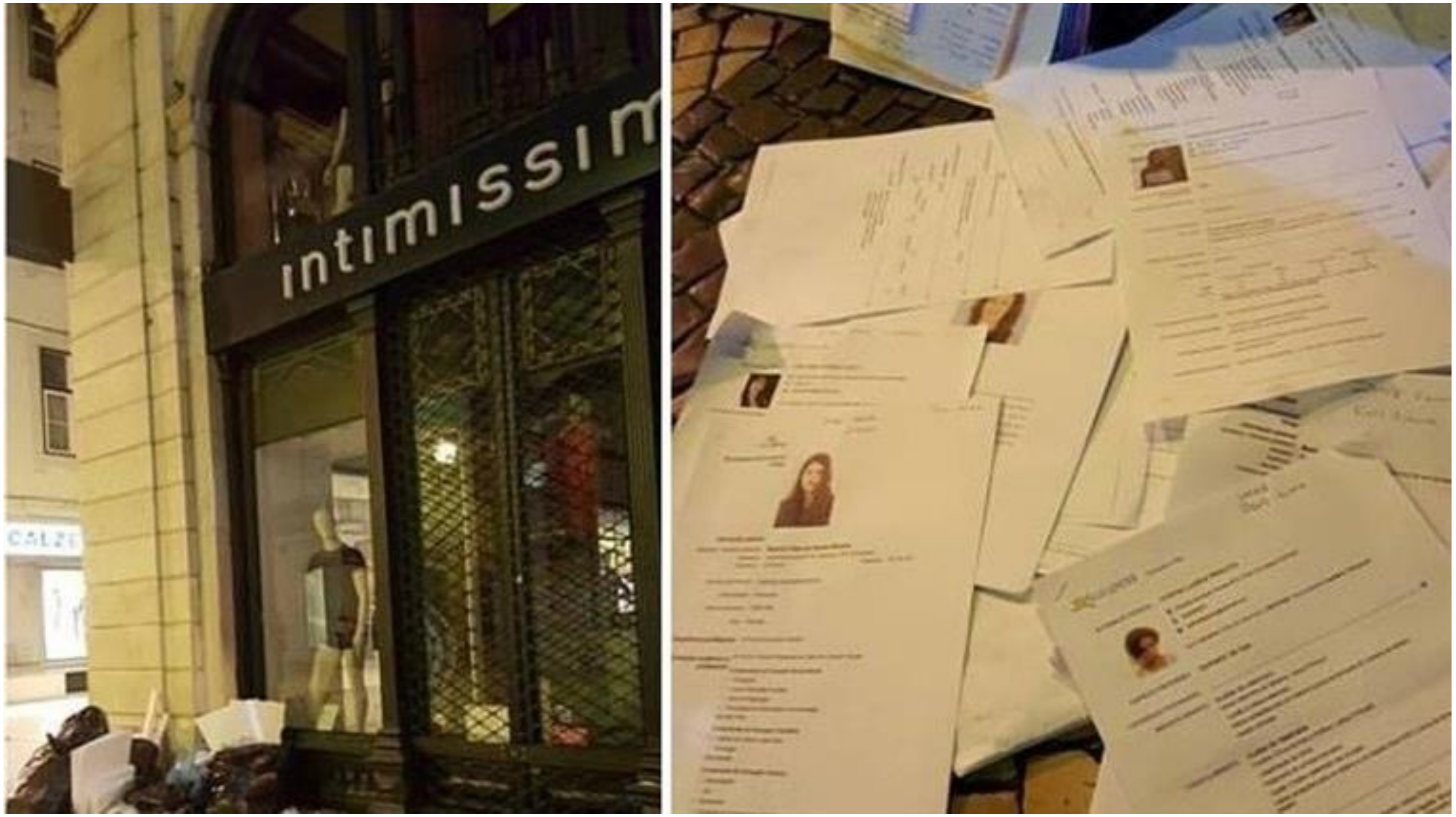
Handling Data and Devices

Data Retention

- All **devices** and **printed materials** must be **destroyed** prior to **disposal**
  - "Dumpster diving"
    - Obtaining the contents of a "dumpster" to **gain unauthorized** access to sensitive information
      - It is not illegal - it has no owner
      - It is perhaps a trespass - but you won't get your data back!
      - Consider safe disposal, using means that may involve security guards, or companies certified to do so!

Handling Data and Devices

Data Retention



https://sol.sapo.pt/noticia/480881

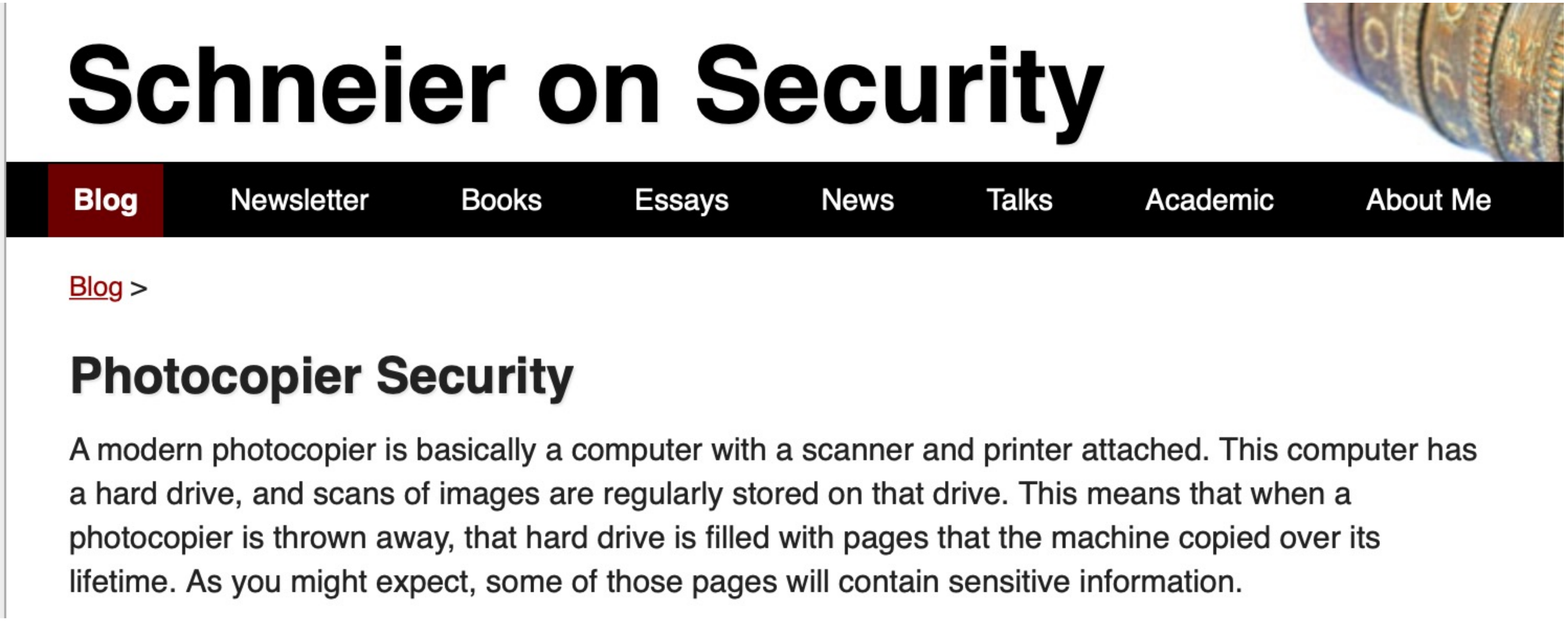
Data Remanescence

Data Retention

- Magnetic and memory devices often retain digital data after normal "erasure" processes
  - CPU registers, cache memory, RAM
  - HDD, backup tapes, flash memory, solid state drives (SDD)
- Must be securely erased (or can be recovered by some unauthorized persons)
  - Rewritten - once or several times
  - "Zeroed" - all bits to zero
  - "Degaussed" - removal of magnetic pulses
  - Physical destruction

Data Remaniscence

Data Retention



Schneier on Security

Photocopier Security

A modern photocopier is basically a computer with a scanner and printer attached. This computer has a hard drive, and scans of images are regularly stored on that drive. This means that when a photocopier is thrown away, that hard drive is filled with pages that the machine copied over its lifetime. As you might expect, some of those pages will contain sensitive information.

https://www.schneier.com/blog/archives/2017/01/photocopier_sec.html
https://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

Secure Erase

Data Retention

- Tools you can use to safely erase digital content:
  - Secure Erase (HDDErase.exe - UCSD) - securely erases the entire disk
  - Darik's Boot and Nuke (DBAN) - Linux distribution - entire disk
  - SDelete Tool - file-level
  - Linux "shred -u" tool - file-level
- Physical Shredding
  - "Shredder" for paper or optical disks
  - Burning, crushing, drilling, etc.

https://dban.org

DBAN

2022 | 2023

Network and Information Systems Security

Asset Security

Carlos Serrão

carlos.serrao@iscte-iul.pt

iscte INSTITUTO UNIVERSITÁRIO DE LISBOA