Thor’s Quick Sheets – CISSP® Domain 2

Contents

The Information Life Cycle

Data Acquisition: The information is either created or copied from another location. We make it useful, index it, and store it.
Data Use: How to ensure the data is kept confidential, the integrity is intact, and available when needed (The CIA triad).
Data Archival: Retention is required by law, or the data will be used later. Archival vs. backup.
Data Disposal: How do we dispose of the data properly when it is no longer useful and required?

Data Classification Policies

Labels: Objects have Labels assigned to them. The label allows subjects with the right clearance to access them. Labels are often more granular than just "Top Secret"; they can be "Top Secret – Nuclear."
Clearance: Subjects have Clearance assigned to them. It is a formal decision on a subject's **current** and future **trustworthiness**. The higher the clearance = more in-depth the background checks should be (in the military, not always in the corporate world).
Formal Access Approval: Document from the data owner approving access to the data for the subject. Subject must understand all requirements for accessing the data and the liability involved if compromised, lost, or destroyed. Appropriate Security Clearance is required as well as Formal Access Approval.
Need to Know: Just because you have access does not mean you are allowed the data. You need to have a valid reason for accessing the data. You can be terminated/sued/jailed/fined if you do not have one.
Least Privilege: Users have the minimum necessary access to perform their job duties.
Military Classifications:

- **Top Secret (TS): Exceptionally grave damage.** Weapon blueprints, theater or war plans, espionage data.
- **Secret (S): Serious damage.** Troop plans, deployment plans, plans not included in TS plans, reports on shortages or weaknesses.
- **Confidential (C): Damage**. Intelligence reports, operational or battle reports, mobilization plans.
- **Unclassified (U):** Available upon request, does not need a classification or has been declassified.

Private Sector Classifications:

- **Confidential: Exceptionally grave damage.** Proprietary information, trade secrets, source code, anything that gives us a competitive advantage.
- **Private: Serious damage.** PHI, PII, financial data, employee data, payroll.
- **Sensitive: Damage.** Networking diagrams, IP assignments, system, and software specifics.
- **Public:** Websites, advertisements, any information we make publicly available.

Sensitive Information and Media Security

Sensitive Information: Any organization has data that is considered sensitive for various reasons. We want to protect the data from Disclosure, Alteration, and Destruction (**DAD**).
Data has 3 States: We want to protect it as well as we can in each state.

- **Data at Rest** (Stored data): Data on disks, tapes, CDs/DVDs, USB sticks. We use disk encryption (full/partial), USB encryption, tape encryption (avoid CDs/DVDs). Encryption can be hardware or software encryption.
- **Data in Motion** (Data is being transferred on a network): We encrypt our network traffic, end-to-end encryption both on internal and external networks.

- **Data in Use** (We are actively using the files/data, it cannot be encrypted): Use good practices; clean desk policy, print policy, allow no ‘shoulder surfing,’ the use of view angle privacy screen for monitors, locking computer screen when leaving the workstation.

Data Handling: Only trusted individuals should handle our data; we should also have policies on how, where, when, and why the data was handled. Logs should be in place to show these metrics.

Data Storage: Data should be kept in a secure, climate-controlled facility, preferably geographically distant or at least far enough away that potential incidents will not affect that facility too. Many older breaches were from bad policies around tape backups. Tapes were kept at the homes of employees instead of at a proper storage facility or in a storage room with no access logs and no access restrictions (often unencrypted).

Data Retention: Data should not be kept beyond the period of usefulness or beyond the legal requirements (whichever is greater). Regulation (HIPAA or PCI-DSS) may require a certain retention of the data (1, 3, 7 years, or infinity). Each industry has its own regulations and company policies may differ from the statutory requirements.

Data, System, Mission Ownership, Custodians, and Users

Mission/Business Owners: Senior executives make the policies that govern our data security.

Data/Information Owners: Management level; assigns sensitivity labels and backup frequency. Could be you or a data owner from HR, payroll, or other departments.

Data Custodians: These are the technical hands-on employees who do the backups, restores, patches, and system configuration. They follow the directions of the data owner.

System Owner: Management level and the owner of the systems that house the data. Often a data center manager or an infrastructure manager.

Data Controllers and Data Processors: Controllers create and manage sensitive data in the organization (HR/Payroll). Processors manage the data for controllers (Outsourced payroll).

Security Administrators: Responsible for firewalls, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), security patches, creating accounts, and granting access to the data following the data owner’s directions.

Supervisors: Responsible for user behavior and assets created by the users. Directly responsible for user awareness and needs to inform the security administrator if there are any changes to user employment status, user access rights, or any other pertinent changes to an employee’s status.

Users: These are the data users; user security awareness trained. They need to know what is acceptable and unacceptable, and the consequences for not following the policies, procedures, and standards.

Auditors: Responsible for reviewing and confirming our security policies are implemented correctly, we adhere to them, and provide the protection they should.

Memory and Data Remanence

Data Remanence: Data left over after normal removal and deletion of data.

Memory: Is just 0s (off) and 1s (on); switches representing bits.

ROM: (Read Only Memory) nonvolatile (retains memory after power loss); commonly used for the BIOS.

- **PROM** (Programmable Read-Only Memory)
- **EPROM** (Erasable Programmable Read-Only Memory)
- **EEPROM** (Electrically Erasable Programmable Read-Only Memory)

PLD (Programmable Logic Devices): Programmable leaving the factory (EPROM, EEPROM, and flash memory). Not PROM.

Cache Memory: L1 cache is on the CPU (fastest), L2 cache is connected to the CPU, but is outside it.
RAM (Random Access Memory): Volatile memory. It loses the memory content after a power loss (or within a few minutes). This can be memory sticks or embedded memory.

- **SRAM** (Static RAM): Fast and expensive. Uses latches to store bits (Flip-Flops). Does not need refreshing to keep data, keeps data until power is lost and can be embedded on the CPU.
- **DRAM** (Dynamic RAM): Slower and cheaper. Uses small capacitors. Must refresh to keep data integrity (100-1000ms) and can be embedded on graphics cards.
- **SDRAM** (Synchronous DRAM): What we normally put in the motherboard slots for the memory sticks. DDR (Double Data Rate) 1, 2, 3, 4 SDRAM.

Firmware: The BIOS on a computer, router, or switch; the low-level operating system and config; stored on an embedded device. PROM, EPROM, EEPROM are common firmware chips.
Flash Memory: Small portable drives (USB sticks are an example); they are a type of EEPROM.
SSD Drives: A combination of EEPROM and DRAM, cannot be degaussed. To ensure no data is Readable, we must use ATA Secure Erase and/or destruction of SSD drives.

Data Destruction

Paper Disposal: It is highly encouraged to dispose of ANY paper with any data on it in a secure manner. This also has standards and cross shredding is recommended. It is easy to scan and have a program re-assemble documents from normal shreds.
Digital Disposal: The digital disposal procedures are determined by the type of media. **Deleting, formatting, and overwriting (soft destruction).**
Deleting: Removes a file from the table; everything is still recoverable.
Formatting: Does the same as deleting but it also puts a new file structure over the old one. Still recoverable in most cases.
Overwriting: (Clear) Done by writing 0s or random characters over the data.
Sanitization: Rendering target data on the media infeasible for a given level of recovery effort.
Purge: Removing sensitive data from a system or device to a point where data recovery is no longer feasible even in a laboratory environment.
Degaussing: Destroys magnetic media by exposing it to a very strong magnetic field. This will also most likely destroy the media integrity.
Full physical destruction is safer than soft destruction:

- **Disk Crushers:** They crush disks (often used on spinning disks).
- **Shredders:** Do the same thing as paper shredders do, they just work on metal. These are rare at normal organizations, but you can buy the service.
- **Incineration, Pulverizing, Melting, and Acid:** Used (very rarely) to ensure full data destruction.

Data Security Controls and Frameworks

Scoping: Determining which portion of a standard we will deploy in our organization. We take the portions of the standard that we want or apply to our industry and determine what is in scope and what is out of scope.
Tailoring: Customizing a standard to your organization; <this> standard, but we use <AES 256bit>.
Certification: A system, and the security measures to protect it, meet the security requirements set by the data owner or by regulations/laws.
Accreditation: The data owner accepts the certification and the residual risk. This is required before the system can be put into production.

Data Protection

Digital Rights Management (DRM): Uses technology and systems to protect copyrighted digital media. Encryption – Regional DVDs. Permissions management and limiting access. Serial numbers, limit installations, expiry dates, IP addresses, geolocation, VPN. Copy restrictions: copy, edit, saving, screenshots, screen recording, printing. Persistent authentication and audit trails. Tracking – watermarks or metadata embedded in files.
Cloud Access Security Broker (CASB): On-premises or cloud software between our users and our cloud applications. Monitors user activity, warn admins about possible malicious/dangerous actions, malware prevention, protects against shadow IT, and enforces security policy compliance.
Data Loss Prevention (DLP): Loss vs. leak. Data in use, in motion, and at rest. Network and endpoint DLP.