* **Three Objectives of Cybersecurity Programs (CIA Triad):** 
  + Confidentiality
  + Integrity
  + Availability
* **Confidentiality**:
  + Ensures that unauthorized individuals are not able to gain access to sensitive information.
    - Enforced with firewalls, access control lists, and encryption.
* **Integrity**:
  + Ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally.
    - Enforced with integrity control such as hashing and monitoring systems.
* **Availability**:
  + Ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them.
    - Enforced with fault tolerance, clustering, and backups.
* **Data Breach Risks - Security Incidents**:
  + Occur when an organization experiences a breach of the confidentiality, integrity, and/or availability of information or information systems.
    - Can occur intentionally, accidentally, or due to nature events/disasters.
* **DAD Triad**:
  + Model that explains the three key threats to cybersecurity efforts
    - Disclosure
    - Alteration
    - Denial
* **Disclosure (Data Loss):**
  + The exposure of sensitive information to unauthorized individuals, both intentionally and accidentally. Violation of Confidentiality.
    - Data Exfiltration: When an attacker gains access to sensitive info and remove it from the organization.
* **Alteration**:
  + The unauthorized modification of information and is a Violation of Integrity. Can also be intentional or accidental.
* **Denial**:
  + The disruption of an authorized user’s legitimate access to information. Violation of Availability. Can also be intentional or accidental.
* When accessing threats to your organization’s website, you may apply the DAD Triad in your analysis:
  + Does the website contain sensitive info that would damage the organization if disclosed to unauthorized individuals?
  + If an attacker modified information on the website, would it cause financial, reputational, or operational damage?
  + Does the website perform mission critical activities that could damage the business if an attacker were able to disrupt the site?
* **Breach Impacts:**
  + The potential impact of a security incident can be categorized as risks:
    - Financial
    - Reputational
    - Strategic
    - Operational
    - Compliance
* **Financial Risk**
  + Any monetary damage to the organization, can be direct financial damage such as the cost of rebuilding a datacenter that was physically destroyed, or the costs of hiring forensic analysts to see why the breach happened.
  + Can be more indirect where if an employee loses a laptop with a new secret product design, and another company steals the design, then problems such as increased competition may ultimately lead to financial loss.
* **Reputational Risk:**
  + Security breaches in general may make all stakeholders less confident in the company and its services, along with fearing private user data being leaked.
* **Strategic Risk:**
  + A breach will make the organization less effective in meeting its major goals and objectives.
    - Like how if an employee loses the designs to a product, it will delay the release of the product, and may give competitors advantages in producing a similar product.
* **Operational Risk:**
  + Risk to the organization’s ability to carry out its day-to-day functions.
    - May slow down business processes, delivery of customer orders, etc.
    - Different to Strategic Risk in which operation here is delayed, but not at jeopardy.
* **Compliance Risk:**
  + Occurs when a breach causes an organization to run afoul of legal regulatory requirements.
    - Example: **Health Insurance Portability and Accountability Act (HIPPA)** requires that health-care providers and other covered entities protect the CIA of protected health information (PHI).
      * A data breach will violate HIPPA requirements leading to sanctions and fines.
* **Implementing Security Controls:**
  + An organization analyzes its risk environment and determine the level of protection required to preserve the CIA of their computer information system.
  + **Control Objectives:**
    - Requirements needed to achieve these security objectives.
  + **Security Controls:**
    - Specific measures that fulfill the security objectives.
* **Security Control Categories:**
  + **Technical Controls:**
    - Enforce CIA in the digital space. Includes firewall rules, access control lists, encryption, etc.
  + **Operational Controls:**
    - Include the processes that we put in place to manage technology in a secure manner. These include user access reviews, log monitoring, and vulnerability management.
  + **Managerial Controls:**
    - Procedural mechanisms that focus on the mechanics of the risk management process. These include periodic risk assessments, security planning exercises, and the incorporation of security into an organization’s change management, service acquisition, and project management practices.
* **Security Control Types:**
  + CompTIA divides security into types, based on their desired effect.
    - **Preventive Controls:**
      * Intend to stop a security issue before it occurs. Includes firewalls and encryption.
    - **Detective Controls:**
      * Identify security events that have already occurred. Includes intrusion detection systems.
    - **Corrective Controls:**
      * Remediate security issues that have already occurred. Includes restoring backups after a ransomware attack.
    - **Deterrent Controls:**
      * Seek to prevent an attacker from attempting to violate security policies. Includes guard dogs or barbed wire fences.
    - **Physical Controls:**
      * Security controls that impact the physical world. Includes fences, locks, fire suppression.
    - **Compensating Controls:**
      * Controls designed to mitigate the risk associated with exceptions made to a security policy.
        + **The Payment Card Industry Data Security Standard (PCI DSS)** includes one of the most formal compensating control processes in use today. Includes three required criteria:

**Control must meet the intent and rigor of the original requirement.**

**The control must provide a similar level of defense as the original requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.**

**The control must be “above and beyond” other PCI DSS requirements.**

* + - * + An example is if an important program required for business is only available on an older, security vulnerable operating system. Running this program normally will most likely violate Security Policies. However, a Compensating Control may be to run this program on a machine that is on an isolated network, so that the security requirements are not only met, but improved.
* **Data Protection:**
  + While data most obviously needs to be protected, it is important to consider how and where data is and represented. There are 3 main states:
    - **Data at Rest:**
      * Stored data that resides on hard drives, tapes, in the cloud, or on other storage media.
    - **Data in Motion:**
      * Data that is in transit over a network.
    - **Data in Processing:**
      * Data that is actively in use by a computer system. Includes the data stored in memory while processing takes place.
* **Data Encryption:**
  + Encryption technology uses mathematical algorithms to protect information from prying eyes, both while it is in transit over a network and while it resides on systems. Encrypted data is unintelligible to anyone who does not have access to the appropriate decryption key.
* **Data Loss Prevention (DLP):**
  + System that helps organizations enforce information handling policies and procedures to prevent data loss and theft. They search systems and networks for sensitive information that is unsecured.
    - They can act quickly to block the transmission before damage is done and alert administrators to the attempted breach.
    - DLP systems work in two different environments:
      * **Host-based DLP**
        + Software installed on systems that search for sensitive info and find things like SSN and credit card numbers.
        + Can also monitor system configurations and user actions, blocking undesirable actions, just as blocking USB.
      * **Network DLP**
        + Dedicated devices that sit on a network and monitor outbound network traffic, watching for the transmission of unencrypted sensitive information.

These systems can block the transmission or apply encryption to the transmission before letting it out.

* + - * DLP systems have two mechanisms of action:
        + **Pattern Matching:**

Look for telltale signs of sensitive information, such as the format of an SSN or credit card or find terms such as “Top Secret” or “Business Confidential”.

* + - * + **Watermarking:**

Systems or administrators apply electronic tags to sensitive documents and then DLP systems can monitor systems and networks for unencrypted content containing those tags.

Commonly used in digital rights management (DRM) solutions that enforce copyright and data ownership restrictions.

* **Data Minimization:**
  + Techniques that seek to reduce risk by reducing the amount of sensitive information that we maintain on a regular basis.
    - The best way to achieve this is to simply destroy data when it is no longer necessary to meet our original business purpose.
  + **De-Identification:**
    - If data cannot be completely removed from a dataset, we can often transform it into a format where the original sensitive information is de-identified. This removes the ability to link the data back to an individual, reducing its sensitivity.
  + **Data Obfuscation:**
    - An alternative to De-Identification where data is transformed into a format where the original information can’t be retrieved.
      * **Hashing:**
        + Uses a hash function to transform a value in our dataset to a corresponding hash value. If we apply a strong hash function to a data element, we may replace the value in our file with the hashed value.

Rainbow Table Attack:

Can be used to reverse the hashing of data by hashing a list of possible data values and trying to see if any of the generated hash values match.

* + - * **Tokenization:**
        + Replaces sensitive values with a unique identifier using a lookup table. But the lookup table needs to be available yet secure as it stores the actual sensitive data along with the corresponding identifier.
      * **Masking:**
        + Partially redacts sensitive information by replacing some or all sensitive fields with blank characters, like covering all digits of an SSN but the last 4.