**Security Fundamentals: Policies, Compliance, and Cryptography**

**Security as a Team Effort**

* Security is about **people, processes, and technology**—it requires a culture of shared responsibility.
* Security plans help prepare for risks and focus on **policies, standards, and procedures**:
  + **Policies**: Strategic rules that define what to protect and why.
  + **Standards**: Tactical references that guide policy implementation.
  + **Procedures**: Step-by-step instructions for specific security tasks.

**Compliance and Security Frameworks**

* **Compliance** ensures organizations follow internal security standards and external regulations.
* Non-compliance can lead to fines, penalties, and reputational damage.
* The **NIST Cybersecurity Framework (CSF)** helps manage security risks through three key components:
  + **Core**: Five functions—Identify, Protect, Detect, Respond, Recover.
  + **Tiers**: Measures security performance (Levels 1–4).
  + **Profiles**: Capture a snapshot of a security plan’s current state.

**Security Controls & Information Privacy**

* **Three types of security controls**:
  + **Technical**: Encryption, authentication, firewalls.
  + **Operational**: Training, incident response.
  + **Managerial**: Policies, risk assessments.
* **Information privacy** is about protecting personal data (PII) and ensuring the **principle of least privilege**—users should only have access to what they need.

**Cryptography & Data Protection**

* **Cryptography** secures data by encrypting (scrambling) it and decrypting (restoring) it.
* The **Caesar cipher** (a basic encryption method) shifts letters but is easy to break with brute force.
* Modern cryptographic methods improve security by using **stronger algorithms and better key management** (e.g., avoiding single keys stored in public places).

**Public Key Infrastructure (PKI) and Encryption**

**The Role of PKI**

* Public Key Infrastructure (PKI) secures online data exchange using **encryption and trust mechanisms**.
* It simplifies access to encrypted information while ensuring security.

**Encryption Methods**

1. **Asymmetric Encryption** (Secure but Slower)
   * Uses a **public key** (to encrypt) and a **private key** (to decrypt).
   * Example: A locked box where **anyone can drop items in (public key)**, but **only the owner can open it (private key)**.
   * Secure but computationally slow.
2. **Symmetric Encryption** (Faster but Less Secure)
   * Uses **one secret key** for both encryption and decryption.
   * Example: A **shared key** that both sender and receiver use to access the box.
   * Faster but risky if the key is intercepted.
3. **PKI Combines Both**
   * **Asymmetric encryption** establishes a secure connection.
   * **Symmetric encryption** takes over for speed during ongoing communication.
   * Example: Encrypted messaging apps start with asymmetric encryption for security, then switch to symmetric encryption for efficiency.

**Establishing Trust with Digital Certificates**

* **Problem**: Computers can't distinguish between trusted and untrusted sources naturally.
* **Solution**: PKI uses **digital certificates** to verify identities.

**How Digital Certificates Work**

1. A company wants to secure its website.
2. The company registers its domain and provides **basic details + a public key** to a **Certificate Authority (CA)**.
3. The **CA verifies** the information and encrypts it with its own **private key**.
4. A **digital certificate** is issued, containing the company’s details and the **CA’s signature**.
5. Websites with **valid certificates** signal **trust and authenticity** to users and other systems.

A diagram of a digital certificate

AI-generated content may be incorrect.

**Why PKI is Important**

* Ensures **secure and trusted communication** online.
* Combines **asymmetric and symmetric encryption** for **both security and speed**.
* **Digital certificates** act like **ID badges** to verify authenticity and protect against key misuse.