Name: JAY ARRE TALOSIG
Subject & Section: CTINASSL – COM231
Professor: Mr. Gaudencio Jeffrey G. Romano

Assignment #2: SECURITY POLICY

1. Discuss the information security policy, standards and practices and give example each.

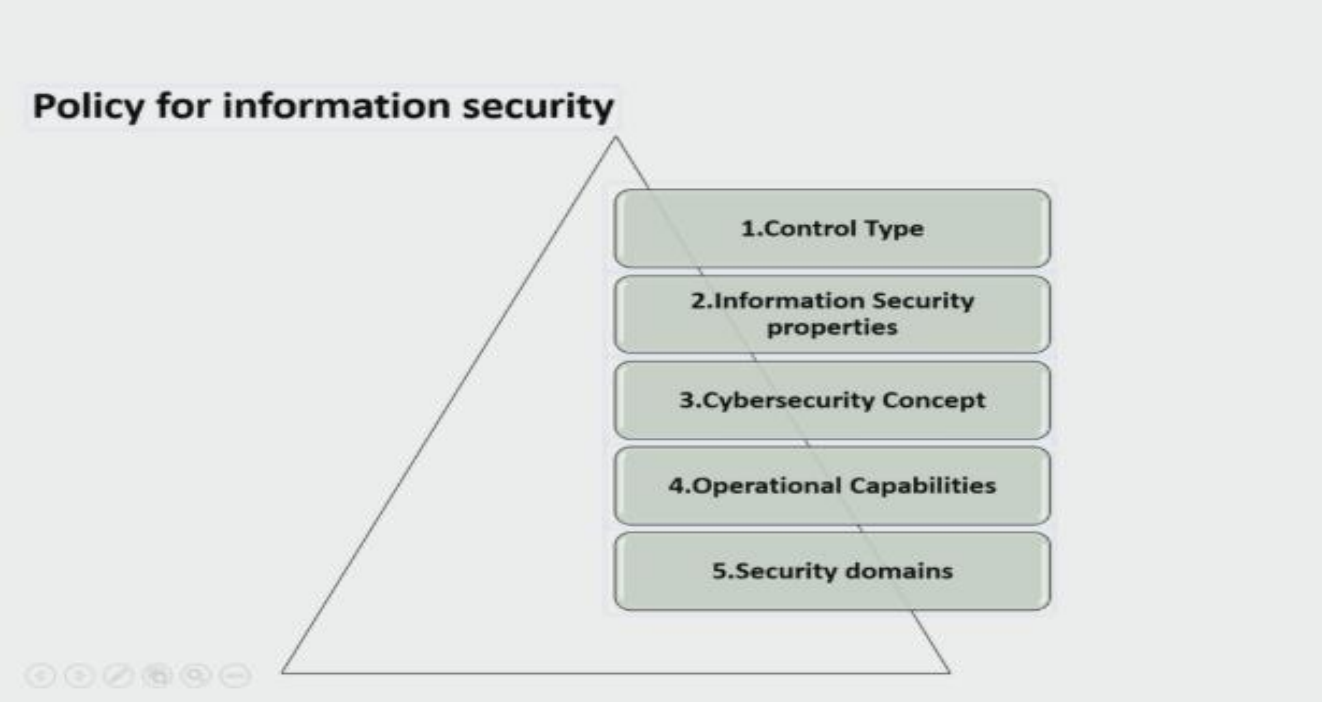
Isipin mo ito bilang isang hierarchy o level ng mga utos sa loob ng kumpanya.

- **Policy (Ang Batas):**
    - Ito ang "General Rules" o ang pinakamataas na utos galing sa management. Sinasabi nito kung *ano* ang dapat mangyari at *bakit*, pero hindi nito sinasabi kung *paano* gagawin step-by-step.
    - **Example:** *Acceptable Use Policy.* Nakasaad dito na ang internet ng kumpanya ay para lang sa trabaho at bawal gamitin sa illegal activities o panonood ng movies.
- **Standards (Ang Requirement):**
    - Ito yung mas detalyado at specific. Sinasabi nito kung anong hardware, software, o technology ang *required* gamitin para masunod ang policy. Mandatory ito at kailangang sundin ng lahat para pare-pareho (uniform).
    - **Example:** Dahil may policy tayo na dapat secure ang computers, ang **Standard** ay: "Lahat ng company laptops ay dapat naka-Windows 11 at may naka-install na CrowdStrike antivirus."
- **Practices / Procedures (Ang Step-by-Step):**
    - Ito na yung "How-to." Dito tinuturo ang tamang paraan o steps para magawa ang trabaho nang secure. Pwedeng guidelines o best practices ito.
    - **Example:** Para masunod ang password policy, ang practice ay: "Tuwing gagawa ng password, gumamit ng phrase na madaling tandaan pero mahirap hulaan, at palitan ito every 90 days."

2. Explain the purpose and structure of security governance.

Ang Security Governance ay hindi lang tungkol sa pag-install ng firewall. Ito ay ang sistema kung paano pinamumunuan at kinokontrol ang security ng buong organization.

- **Purpose (Layunin):**
  - Ang main goal nito ay siguraduhin na ang Information Security ay aligned o tumutugma sa business goals.
  - Para masigurado na sulit ang ginagastos sa security (hindi sobra, hindi kulang) at namamanage nang tama ang mga risks.
  - Para may "accountability" – ibig sabihin, malinaw kung sino ang may kasalanan pag may pumalya at sino ang dapat managot.
- **Structure:**
  - Hindi ito pwedeng galing lang sa IT Dept. Ang structure ay dapat Top-Down. Nagsisimula sa Board of Directors at Senior Executives, pababa sa management, hanggang sa regular employees.
  - Kailangan may basbas ng mga "boss" ang security initiatives para seryosohin ng lahat.

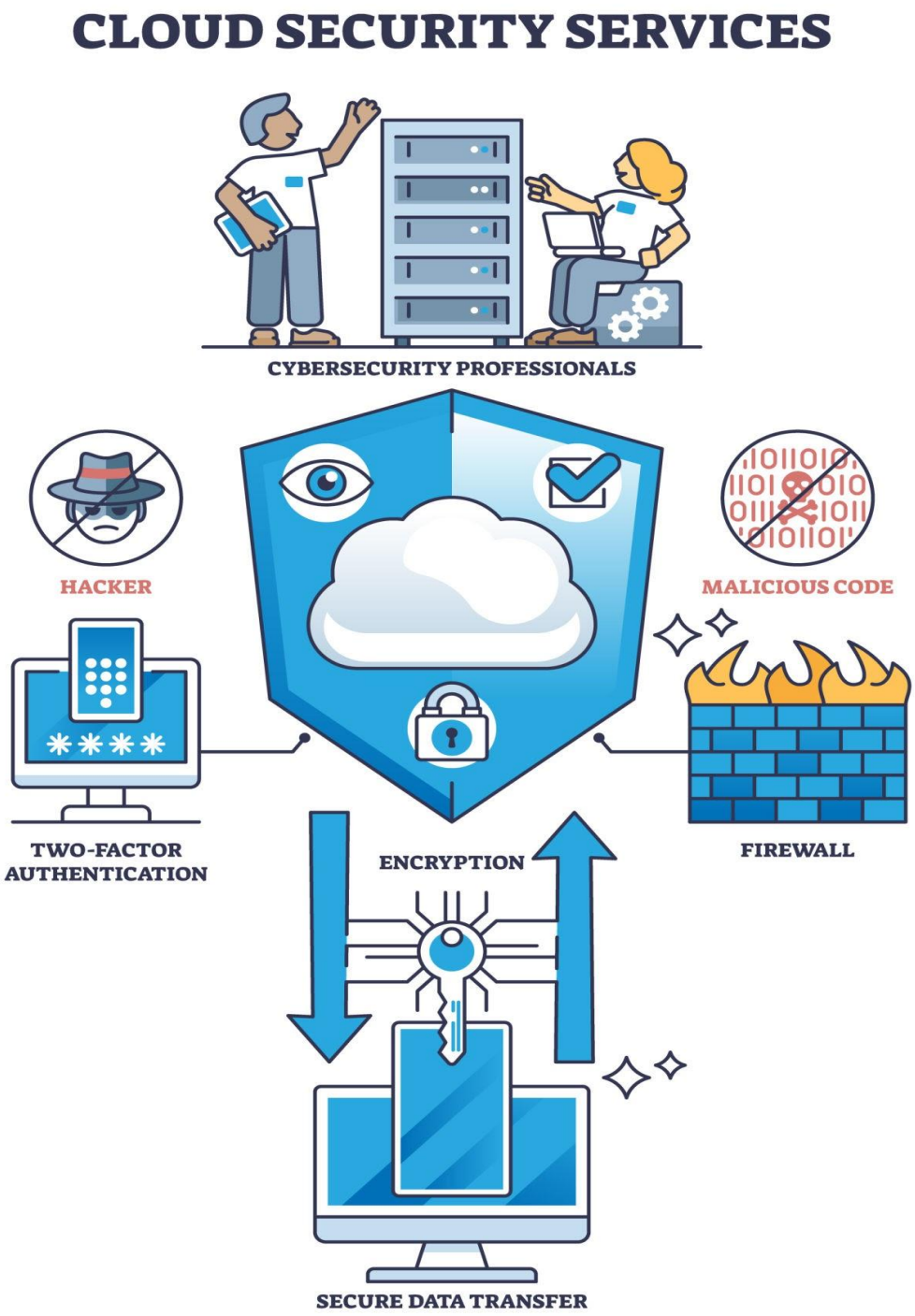


3. Explain the purpose and structure of security governance.

Sa governance, bawat isa ay may role. Hindi pwedeng si IT lang ang bahala sa lahat.

- **Senior Management / C-Level Execs (CEO, COO, etc.):**
    - **Responsibility:** Sila ang nagbibigay ng pondo (budget) at go-signal. Sila ang ultimate na responsable sa batas kapag nagka-data breach.
    - **Example:** Si CEO ang pipirma sa Information Security Policy para maging opisyal na batas sa kumpanya.
- **Chief Information Security Officer (CISO):**
    - **Responsibility:** Siya ang "Captain" ng security. Siya ang gumagawa ng strategy at nagre-report sa management tungkol sa status ng security.
    - **Example:** Si CISO ang magpapaliwanag sa Board kung bakit kailangan bumili ng bagong firewall system.
- **Data Owners:**
    - **Responsibility:** Sila ang mga manager o head ng department na "may-ari" ng data. Sila ang nagdedesisyon kung sino ang pwedeng um-access sa files nila.
    - **Example:** Ang HR Manager ang Data Owner ng "Employee Records." Siya ang magsasabi sa IT kung sinong employees lang ang pwedeng makakita ng sweldo ng iba.
- **Users / Employees:**
    - **Responsibility:** Tayo ito. Ang role natin ay sumunod sa policies at mag-report kung may kahina-hinalang nangyayari.
    - **Example:** Responsibilidad ng employee na huwag i-share ang kanyang password kahit kanino at i-lock ang PC pag aalis sa desk.

4. Explain the role of security blueprint in program development.



Isipin mo na magpapagawa ka ng bahay. Bago ka bumili ng semento at yero, kailangan mo muna ng **Blueprint**. Ganoon din sa security.

- **Ang Role nito:**
    - Ito ang nagsisilbing **Master Plan**. Dito nakadetalye kung paano i-implement ang security controls (tao, proseso, at teknolohiya).
    - Gamit ang blueprint, naiiwasan ang "hula-hula" o bara-barang paglalagay ng security tools. Sinisigurado nito na walang butas (gaps) sa depensa ng kumpanya.
    - Ito ang nagta-translate ng *Policy* (yung gustong mangyari ng management) papunta sa *Technical Implementation* (kung paano ito gagawin ng IT/Security team).
    - Kasama sa blueprint ang plano para sa firewalls, physical security (cctv/guards), training ng tao, at incident response.