**Implementing CIA at the Network Level**

* Read PPT

Ang result ng mga cyber attacks or hacking can cause negative impact sa business. For example, pag nagkaroon ng hacking sa business like banko, magkakaroon ng negative effect ito sa business. May chance na lumipat ng banko si customer kase matatakot na baka mawalan ng pera dahil hindi secured ang system ng banko.

**Authentication Methods**

* Do not read PPT

Authentication is the process of identifying users that request access to a system, network, or device

.

Username and Password- Familiar naman tayo dito, Kadalasan ginagamit natin to sa mga app like Facebook, tiktok, at iba pang app.

PIN- Ginagamit ito sa mga ATM or kapag mag wiwithdraw.

Voice Pattern and Retina Scan- both biometric mehod sya, maganda din syanf authentication method kase hindi sya nahahack. Ikaw lang mismo makakapag bigay nito sa system.

Ginagamit yung Authentication Method para malaman ng system na ikaw ang may ari ng account or device na gusto mong ma access.

**Firewall**

* Read PPT

Ang Firewall ang nag propotect sa system laban sa mga hackers. Firewall ang nagsisilbing pagitan at nagbibigay ng access sa system.

Ang main goal ng Firewall is to prevent unauthorized access sa network.

**Router**

Familiar naman tayo dito sa router, kapag nag patakid tayo ng internet is merong kasamang router, ginagamit sya para ma connect ang internet provider at network at home. Gamit ang router pwede ka mag restrict ng devices na naconnect sa network mo.

Low level of security ang router kase pwede sya ma hack kaya needed na mag add ng additional security layer.

**Encryption**

* Read PPT

Ginagamit yung encryption para hindi Mabasa ng unauthorized person yung sensitive information.

Encyption key is yung ginagamit para ma encrypt and decryp yung data. Example nya is PIN, Password para ma protect si encryption key.

**Proxy Servers and Virtual Private Networks**

* Read PPT (first bullet only)

Ang proxy server ang nasa pagitan ng end user and internet. Ginagamit sya ng mga company para hindi mala access ng certain website si employee. Nalalaman ni proxy server lahat ng record ng website na binuksan ni employee.

VPN secures all your internet traffic and encrypts it for extra security and privacy. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

**Intrusion Detection System**

intrusion detection system (IDS) is software and/or hardware that monitors system and network resources and activities and notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.

For example may nag send sayo ng email na may lamang virus. I sesend ng router yung email kay IDS at Firewall kapag Nakita ng security team na may threat mag sesend sya ng signal kay firewall na iblock para hindi makapasok yung treath sa network .

**Implementing CIA at the Application Level**

Eto naman yung mga ginagawang security measure para maprotektahan yung application na gingamit.

**Authentication Methods**

Almost similar naman ito dun sa kninang na discuss.

For example Ginagamit yung Two-factor authentication para withdraw ng pera sa bank

Kailangan mo ma present yung mismong card (something that you have) and a PIN (something that you know) para makapag withdraw.

**User Roles and Accounts**

Ibig sabihin each employee ay limited ang access sa kanyang trabaho. Hindi pwede ma access ng employee ang data na hindi naman sakop ng kanyang trabaho. Pag finance department ka yun lang ang ma aacess mo, hindi mo pwde ma access ang Hr.

**Data Encryption**

Same lang den sya nung kanina kailangan yung mga department na may sensitive data is encrypted para ma protect sa unauthorized user.

**Implementing CIA at the End-User Level**

Eto naman yung mga kailangan gawin ng mga end-users. Maaring ang maging dahilan ng mga hacking or cyber attacks ay mismong nasa loob ng network or mga employee na gumagamit nito. Kaya kailangan alam ng isang tao yung security measure para maiwasan yung mga cyber attacks

**Security Education**

Eto yung mga sample question

**Authentication Methods**

Kung available ang ibang security aside sa password pwede natin sya gamitin para mas secured. For example sa device, pwede fingerprint na lang ang gamitin instead na password kase hindi ito basta basta nalalaman or nagagaya ng iba.

**Antivirus software**

Kailangan yung mga ginagamit naten na device is may naka install na anti virus and kailangan ina update din sya para maiwasan yung mga malware.