C - confidentiality ensures only approved users have access to the information  
I - integrity ensures the information is unaltered  
A - Availability ensures the info is accessible

(info on a need to know basis)  
  
AAA

Authentication - the act of ensuring the credentials provided are correct

Authorization - grants permission for a user to take a particular action

Accounting - creates a record that is preserved of who accessed the network, what resources they accessed and when they disconnected from the network  
  
  
Security controls –  
  
Deterrent controls - deterring actions that could cause a breach such as warning a user when a download is suspicious or not from a trusted source  
Preventive controls - not allowing downloads unless from an admin

Detective controls

Compensating controls   
Corrective controls   
Directive controls   
  
  
DID - Defense in depth  
  
Threat actors  
  
Unskilled Attackers - individuals who want to perform attacks yet lack the technical knowledge to carry them out  
  
Using easy to use tools that are freely available or can be purchased at a low cost to perform sophisticated attacks

Shadow IT - The process of bypassing corporate approval for technology purchases

The employee is often ethical but it often weakens security  
  
Organized Crime - A threat actor whose motivation is usually financial

Insider threat - a person with intimate knowledge of a company's inner workings, motivation could be blackmail, revenge or financial, these attacks can be hard to recognize as they already often have clearance into administrative systems or have access to credentials.

Hacktivists - threat actors motivated by ideology or political motivations  
Attacks are usually not financially motivated, often only hacking into websites with the intent of changing its contents as a statement or deleting information  
  
Nation State Actors - Government sponsored hackers for launching attacks against other nations (infrastructure, military systems) often involved in multiyear campaigns targeting highly sensitive proprietary information  
  
APT - a new class of attacks that use innovative tools that silently extract data over a long period of time  
  
Brokers - similar to organized crime, the difference being   
  
Vulnerability - a weakness of a system ie the possibility of being attacked through a certain attack vector, or an update that breaks old code.  
  
Zero day vulnerability - a vulnerability that is found by a threat actor before anyone knows ith exists - prevention includes air gapping your systems either through a restrictive firewall or by physically disconnection your systems to the public internet  
  
Impact of attacks - A successful attack always results in several negative consequences, it may make the systems inaccessible, data can be destroyed, exfiltrated (leaked) deleted (purposefully) or utilized for identity theft.  
  
Defending against attacks - Frameworks and regulations of data security, (NIST Framework)   
  
Regulations - Most organizations follow multiple data safety regulations, either industry standard regulations, or government mandated regulations, companies must follow these or they could face litigation from disgruntled users  
  
Benchmarks/ secure config guides - distributed by hardware manufacturers and