**NBNB This section is in exam**

**Challenges to securing information**

There can never be a blanket approach to cyber security.   
There are so many different types of attacks.  
It much harder to defend against attacks, than actually attack

**Todays attacks**

POS directed attacks.  
-Card scrapers/readers on payment machines.

Healthcare  
-Medical and financial information about patient and family used for identity theft.  
-Can be used for billing fraud and purchasing drugs for resale.

Home wifi  
-If you get in the wifi, you can get all network activity on your wifi.

Vehicle vulnerabilities  
-Jamming

Airplane vulnerabilities  
Air jacking: getting access to flight system

Email  
-spam

**Difficulties in defending against attacks (NB, we will need to give this stuff in exam)**

Universally connected devises  
-Increased points of entry, weakest link

Increased speed of attacks  
-Quicker attacks, result in your computer not being able to react fast enough.

Greater sophistication of attacks

Availability and simplicity of attack tools  
-Script kitties, can buy scripts ect

Faster detection of vulnerabilities  
-There are more vulnerabilities that exists these days

Delays in security updating

Weak security updates distribution

Distribution attacks

User confusion

**Information Security**

Used when creating defenses for computers.

**Understanding Security**

Security: The necessary steps to protect a person or property from harm  
-eg Alarms, fences, protection form natural forces (storms)

Security is inversely proportional to conveniences  
-ie Increased security = decreased convenience  
-This is bery important to note when creating a security system for a business, as if its extremely inconvenient, people will do very unsecure things.

**Defining Information Security (NB for exam)**

Information Security (Need to know: This is definition)  
-Task of securing information in a digital format  
-Ensures protection measures are properly implemented  
-Protects information with value to people and organizations  
  
Three protections that must be extended (CIA) (**NB for exam – apply in use case)**  
-Confidentiality: Message only viewed by intended parties  
-Integrity: Original message not influenced  
-Availability: Must always be accessible.

In addition to the CIA triad, another set of protections must be implemented: (**NB, know these 5 things, for 5 marks)**  
-Authentication – keys: We try verifying who you are.  
-Authorization - keys: Verifying what you have access to.  
-Accountability – keys: Audit trail to determine who has done what  
-Integrity - hashing: Original message not influenced  
-Confidentiality keys: Message only viewed by intended parties  
For each of the above, we need keys (or hashing for integrity).  
  
-We don’t need to know this, but can help with answering Q:  
These are private and public keys: This is for encryption and decryption. This can be used to explain how this gives you eg Confidentiality: Even if user X gets access to the information, they wont be able to read it as they don’t have a private key.

Everyone has a public key (to lock)  
But not everyone has the private key.

With hashing, even if someone gets message and decrypts it, then rehashes it, the end hashing result will be different allowing you to see its been tampered with and should be disregarded.

Information is in 3 layers  
  
1. Policies and procedures: There are no blanket approach, but there are approaches that can meet information standards. This is important as the standard is a credible source and is trusted.   
2. People: The biggest weakness. You cant control what people give away  
3. Products

**In exam, you can give eg layers, or 5 things or convenience vs security: As long as you give 5/10 marks worth of facts, can do any.**

**NB**  
Vulnerability: How can get access to asset (whole)  
Threat Agent: Thief  
Exploit: How you exploit vulnerability eg go through whole  
Risk: Your scooter can be stolen  
Asset: Scooter

Options when dealing with risk (**NB When speaking about risk, need to know how to deal with that risk. Also must know how to define in case of information security)**  
Eg Risk: car accident  
-Risk Avoidance: You can avoid the risk, how to ensure the risk doesn’t happen eg Not drive  
-Risk Acceptance: You accept the risk can occur, but still proceed. This is when the ramifications aren’t bad or the risk is acceptable for reward eg You do drive  
-Risk Mitigation: Ensuring there is least amount of damage can occur eg Driving a car instead of a bike, as less injury  
-Risk Deterrence: Preventing risk from happening eg When driving, you see someone’s going to hit you, you swerve.