Types of attackers

**Amateurs**

Inexperienced **hackers who use existing tools or instructions found on the internet   
 to launch attacks**  (also called ***script kiddies***)  
 **hackers**   
 they break into computer systems or notworks to gain access  
 depending on the intent they are classified into:  
 - **WHITE hat attackers** **identify any weaknesses so that the security of a system or   
 network can be improved, done with permission**  
 - **GRAY hat attackers**  
 **they will report the weakness only if it coincides with they agenda or they public the weakness on internet** - **BLACK hat attackers**

**Take advantage of any vulnerability for illegal personal, financial   
 or political gain**

Organized hackers

**Organization of cyber criminals, hactivists, terrorists and state-sponsored hackers.**

Highly sophisticated and organized and may provide cybercrime as a service to  
 others  
  
 hacktivists = make political statements to create awareness about issues  
 state-sponsored = gather intelligence or commit sabotage on behalf of their  
 government

Internal and external threats

Internal  
  **employees, contract staff or trusted partners can accidentally or intentionally**:  
 - mishandle confidential data

- facilitate outside attacks by connecting infected USB, into organization PC

- invite malware onto the organization network by clicking on malicious   
 emails or websites

- threaten the operations of internal servers or network infrastructure   
 devices

External

**Amateurs or skilled attackers outside of the organization**:  
 - exploit vulnerabilities in the network

- gain unauthorized access to computer device

- use social engineering to gain unauthorized access