

**BCIS 5740**

**Information Security Management**

**Class Activity 1**

**Submitted to: Prof. Obi Ogbanufe**   
  
**Submitted By :**   
**Preeti Chaudhry - 11559290**

**Risk** - Risk is the probability of exposure or loss resulting from a cyber-attack data breach on your organization. There are various types of risks in cyber threat.

There are various types of cyber threats -   
  
- Ransomware: It spreads through phishing emails that contain malicious attachments. When you download an attachment and click there, you’ll get caught in that trap.  
  
- Data Leakage: Data leakage, also called information leakage, refers to passage of information from inside the organization to a destination outside its secured network.  
  
- Hacking: Hacking refers to the misuse of devices like computers, smartphones, tablets, networks to access private information illegally.  
  
- Insider threat: An insider threat is something that originates from within the organization. When some insider person sends some information to the wrong outside information.  
  
**Social Engineering** - It’s the broad range of malicious activities accomplished through human interactions. Social engineering is the psychological manipulation of people into performing some actions. In short, we can call social engineering as broad range of malicious activities which is done by human activities.  
  
**Confidentiality –** It means that some secret information is protected from unauthorized disclosure.Confidentiality involves some set of promises or rules that will come into execution through confidential agreements that limit access to information for particular people.  
  
**Authenticity –** Authenticity means that you’re the true person who holds your own identity, personality, regardless of the pressure you’re under to act otherwise. It’s kind of authentication to assure that you’re the true person who’s going to access this data and information which is stored in the network.

**Integrity –** The term integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.