1.
    - Confidentiality- we want our own privacy and want to limit what others can see about us
    - Integrity- we want to know that the information given to us isn't changed and stays true to its meaning
    - Availability- We want to be. Able to access the information at any time
2. The term authentication is to make sure that the person is who they said they are
3. Multi factor authentication is using more than one method to determine who someone is
4. Role based access control is when one is only allowed to access information only available to the roles they were given
5. The purpose of encryption is to keep information or data hidden and only available to those with proper keys to access the data or information
6. Pretexting is when an attacker calls for help pretending to be someone else and acts like they have trouble logging in while giving out personal information just to acquire the password. It is a threat because you can get into one's personal accounts just by knowing their personal information.
7. Backups create a copy of whatever that can be reached in the future in case software fails or data corruption occurs, and good components of a backup plan is knowing what information needs to be backed up, having a copy of the backed up data stored elsewhere and testing the backed up data.
8. There are two types of firewalls, hardware, or soft wall. A physical device that filters or refines packets. Soft wall acts like a bouncer that picks off packets as they come to the computer
9. –
10. Physical security is keeping the hardware safe and secure