- Securing Individual Systems
  - Redundant Array of Independent Systems (RAID)
    - Multiple "levels" of hardrives
      - RAID0 increases speed
        - Need a minimum of two drives
        - AKA Striping
        - If you lose a drive, you lose all data
      - RAID1 Increases Integrity
        - Mirroring copies data across all dirves
      - RAID2 Does Both
        - Uses a technique known as parity
          - EX: SUPER DUMBED DOWN EXAMPLE OF PARITY => We know that 1 + 2 = 3 but if I took out a number it becomes a trivial algebraic equation (x + 2 = 3). This is essentially what is done with data on a RAID drive that uses parity
        - Requires a dedicated parity drive to perform parity calculations from at least two other drives
      - RAID 5 Distibutes Parity values across all drives
        - Cannot lose more then on drive
        - Need a minimum of 3 drives
      - RAID 6
        - Need a minimum of 4 drives
        - Can lose more then one drive
      - RAID 0+1
        - Mirror of stripes
      - RAID 10
        - Stripe of mirrors
    - Network Attached Storage (NAS)
      - Dedicated device with volumes for sharing
      - File Level
    - Storage Area Network (SAN)
      - Method of transforming files
      - Best used over fiber channel
        - Super expensive
        - Requires a host based adapter (HBA) that runs its own language called fiber channel
      - iScsi
        - Poor mans version
        - Uses existing network to transfer files
        - Initiator goes out and looks for hard drives
      - Block Level
  - Physical hardening
    - Optical Medai
      - Can be managed on the user or system level
      - Can be managed in AD
      - Usually want to disable things like autoruns
    - Data Execution Policy
      - You may (probably will never have too realistacly) disable specified executables from executing via system settings
    - Ports
      - Serial Ports should be turned off
      - Can be managed from the BIOS
  - EMI, RFI, ESD
    - Radio Frequency Interference
      - If technology emits radiation in radio frequency range interference can be generated
      - Protection
        - Isolation
        - Shielding
        - Separate circuit
    - Electro Static Discharge
      - Static + Circuit Board = Destruction
      - Protection
        - Keep techinician and electronic at same potential
        - ESD Wriststrap
        - Usually used in storage media to protect from static discharge
        - Anti ESD Circuitry
  - Host Hardening
    - Services
      - Disable unecessary services
    - Default Passwords
      - Do not ever use default passwords
      - Some of the worst bot net attacks occured on IOT devices
    - Active Directory
      - Check OU's and groups
      - Check for guest use accounts and disable them
      - Least Privilege is your friend
    - Patch management
      - Patching in an enterprise environment is a different beast then normal patching in home
      - Monitor for patches coming out
      - Test patches before deploying
      - Try to see if you even need the patch - some patches are minor fixes that do not really fix security bugs. Take this with a grain of salt however
    - Anti-Malware
      - Monitor logs
        - Check DNS
        - Check process interactions
        - Check signatures against third party databases
      - Train staff
    - Host Firewalls
      - By default only as good as user monitoring
      - Best to whitelist applications and blacklist known bad
  - Peripherals
    - Bluetooth attacks
      - Bluejacking - Occurs when someone is able to connect and send data to any bluetooth enabled device
      - Bluesnarfing - Occurs when some is able to connect and steal data from any bluetooth enabled device
      - Distance plays a role here
    - WPS
      - Don't use this - it is really REALLY easy to crack passwords including WPA2 passwords with this feature installed
    - Keyboards, mice etc. Must be patched.
    - SD Protocol enabled devices scan become access points
    - Be careful for rogue USB devices
  - Host Threats
    - Spam
      - Usually just an annoyance
    - Phishing
      - More targeted then normal spam
      - Spear phishing is even more targeted then phising
    - Spim
      - Spam via instant mesaging
    - Vishing
      - Phishing over VOIP
    - Privilege Escalation
  - MITM
    - The ability to attack clients by staying in the middle of session
    - An easy (but loud) method to use is ARP spoofing
      - See all unencrypted traffic
      - Must be on the network
      - Loud, generates a ton of ARP broadcasts
    - WEP is susceptible due to weak cryptographic protocols
    - Near-Field Communication is susceptible but attacker must be very close
    - Domain Hijacking
      - Attacker claims a recently expired domain and requests money for it
    - DNS Redirect
      - Poison client cache to forward common requests to a malicious server
    - Downgrade attack
      - Downgrade secure protocols to insecure protocols
    - Replay attack
      - Take authentication mechanism (I.e. cookie/token) and reuse it for authentication to session
  - Denial of Service
    - Volume Attack
      - Examples
        - UDP Flood
        - Ping flood
      - Doing a lot of requests
    - Protocol attack
      - Exploit unhandled errors to slow down response
      - SYN Flood
        - Send a bunch of SYN requests without waiting for ACK
    - Application attack
      - Exploit a application flaw
      - Slow loris
        - Initiate connection then do not respond
    - DDOS
      - Attack with several computers
      - Popular with botnets
  - Resiliency
    - Scalability
      - Ability to distribute work across nodes
    - Elasticity
      - Ability to scale according to demand
      - EX: Amazon S3
    - Redudancy
      - Add the same exact thing for good measure
      - EX: Multiple Domain Controllers
    - Non-Persistance
      - Don't save anything
      - Snapshots
      - Known state
      - Live boot
      - Roll back
  - Hardware/Firmware Security
    - Fulldisk Encryption
      - Trusted Platform Module: Asynchronous encryption method between motherboard and disk. If TPM is turned on and disk is separate from motherboard, data cannot be accessed
      - Self Encrypting Drive (SED)
        - At bootup, data is encrypted with symmetric key (password)
    - Hardware Security Module (HSM)
      - Can store most signed keys
      - Used a lot with web servers
      - Used where a lot of signing going on
    - Secure boot
      - TPM 2.0 feature - As soon as system boots up, all application must be signed
      - Secure supply chain
        - EX: Apple
      - Creates what is known as a hardware root of trust