**Computer and Network Security Week 1**

* Module 1: Intro to Security
  + Define Information security and why it's important
  + Explain the Impact of attacks
* What is Information Security?
  + Security is to be free from danger, the process that achieves that freedom
  + The more secure something is, the less convenient it may become to use. Users are usually required to perform additional tasks to abide by the security policies
  + Information Security describes the tasks of securing digital information whether it is:
    - Manipulated by a microprocessor
    - Preserved on a storage device
    - Transmitted over a network
  + 3 Types of Information protection (CIA Triad):
    - Confidentiality : Only approved individuals may access information
    - Integrity: Ensures information is correct and unaltered
    - Availability: Ensures information is accessible to authorized users
  + Security Layers
    - Heart: Information (CIA Triad, either transmitted, stored, processed)
    - First Layer (Products) : Hardware and Software ensure security
    - Second Layer (People) :
    - Third Layer (Policies and procedures)
  + Threat Actors
    - An individual or entity responsible for cyber incidents against the technology equipment of enterprises and users. Attacker
    - Financial crime is divided into Individual users, enterprises, and governments
    - Black Hat hackers:
    - White Hat Hackers: Testing, finding holes in security
    - Gray Hat Hackers: Illegal form of white hat hacking
  + Script Kiddies
    - Are individuals who want to perform attacks yet lack knowledge to do it. They download freely available automated attack software and use it to attack
  + Hacktivists
    - Individuals motivated by ideology
    - Usually attack by hacking a website and changing its content as a political statement
  + State Actors:
    - Governments employ their own state sponsored attackers for launching attacks on their foes. Dangerous due to funding
    - Advanced Persistent Threat (APT) is a new class of attack, persistently attacking security hole
  + Insiders:
    - Employees, contractors, and business partners can pose and insider threat of manipulating data from the position of a trusted employee
    - 6/10 enterprises reported being a victim of insider attacks in 2019
    - Focus of insiders:
      * Intellectual property: 43%
  + Other Threat Actors
    - Brokers
    - Competitors
    - Shadow IT: installing own tech in frustration of slow pace, violating company policies
    - Cyberterrorists
    - Criminal Syndicates
  + Vulnerabilities and Attacks
    - Social engineering: one of the most successful attacks, does not even exploit tech vulnerabilities. Phone scams, etc
    - A vulnerability is the state of being exposed to the possibility of being attacked.
    - Cybersecurity vulnerabilities are categorized into platforms, configurations and third-party patches, and zero-day vulnerabilities
      * Platforms
        + A system that consists of the hardware device and an OS that runs software
        + All platforms have vulnerabilities to some degree, some more serious such as:

Legacy platforms

On-premises platforms

Cloud platforms

* + - * Configuration settings:
        + Not properly implemented
      * Third Party
        + Almost all businesses use external entities known as third parties
        + Vendor management is used to monitor and manage interaction with third parties
        + Connectivity between org and third party is system integration
        + Weakest link principle:
      * Patches
        + Updates and patches are important but can cause vulnerabilities:
        + Difficulty patching firmware
        + Few patches for app software
        + Delays in patching Oss
      * Zero-Day
        + Vulnerabilities can be exposed before anyone even knows they exist
        + Provides zero days of warning
        + Extremely serious vulnerabilities
  + Attack vectors
    - A pathway or avenue use by a threat actor to attack
    - Social engineering Attacks :
      * A means of eliciting information by relying on weakness of individuals
      * Psychological principals
        + Attackers use a variety of techniques to gain trust
        + Provide reason, project confidence, evasion and diversion,
      * Impersonation
      * Phishing: email or announcement that falsely claims to be an enterprise to trick user into giving private info
        + Spear Phishing: Sending millions of emails to everyone, Whaling: targeted groups of people, Vishing: Through a phone call, Smishing: SMS phishing
      * Redirection:
        + attacker directs user to fake lookalike site
        + use sites with similar spelling, called typo squatting
        + Pharming is an attempt to exploit how a URL is converted to its IP address
      * Spam
        + Unsolicited email
        + Spim is the same but in instant message
      * Hoaxes: False warnings
      * Watering hole attack is directed to a smaller group of specific individuals with spam
      * Physical Procedures: Dumpster diving, tailgating, shoulder surfing
    - Impact of attacks
      * Data loss – destroying data
      * Data exfiltration – stealing data
      * Data Breach – stealing data to disclose
      * Identity theft
      * Effects on the Enterprise: Availability loss (systems not available) Financial loss, (Reputation loss)