**Elements of Security**

Confidentiality

Integrity

Authenticity

Availability

**Security attacks**

A computer worm

-Program that replicates itself to infect other computers

**Damages done by computer worms**

-Bandwidth consumptiom

-Stops Anti-Malware actions

-Turns off Safe Modes

-In cases of Windows Operating Systems, it turns off auto-update

**Computer virus**

-Program that hides itself within a harmless program that reproduces itself to perform actions such as destroying data

**Damages done by the computer virus**

-Corrupting files

-Computers slow down

-Takes over the OS functions

**Spyware**

-Program that designed to collect information about an individual or company without their consent. Can sometimes be used to access to one’s computer without being noticed

**Damages done by Spyware**

-Collecting personal information

-Installing unsolicited software

-Changing computer settings

-Slowing down internet connection

**Trojan**

-Program that misleads users of what it truly does.

**Damages done by Trojans**

-Crashing the computers

-Deleting files

-Corrupting data

**Security Breaches**

-Situation where individual or company data is released to a treachorous entity with or without intention. This can lead to cyber blackmail, identity theft

**Phising**

-Obtaining personal information by appearing to be a legitimate source

Can be through email attachment

**Identity Theft**

-Obtaining the computer details or company details and assume their identity to commit cyber crime after the crime is committed, they are untraceable

**Prevention**

-Be mindful of email attachment

-Use anti-virus and anti-malware software

-Don’t respond to unsolicited requests

**Harassment(cyberbullying)**

-Situation where an attacker post negative comments about a company that can ruin its reputation

**Prevention**

-Do not respond immediately

-Get the authorities involed

**Cyberstalking**

-Situation where an attacker does acts of false accusations and defamation

**Prevention**

-Have physical accesss of computers

-Always log out of programs before leaving

-Protect your passwords(Keep on changing them)

-Keep your security software updated

**Cyber Attacks**

-Aim to destroy information systems, networks etc

**Password Attacks**

-Use strong passwords

**Guidelines to make passwords**

-Make it easy for you but difficult for others to guess.

-Use both uppercase and lowercase letters.

-Include numbers,symbols and special characters

-Make it a long password

-Update it regularly

**Denial of Service attack(DoS)**

-Aim to make a network unavailable to its intended users.

**Damages of DoS attacks**

-Slow network performance

-A specific website cannot be accessed

-No website is accessible

-A large amount of spam emails are received

**Passive Attack**

-An attack that is done to find the vulnerabilities of a system and take harmful actions at a later stage.

**Penetration testing**

-This is an attack that is done to discover the vulnerablities of a system, take advantage of them to understand the impact of an actual attack. It is quite useful for setting up precautionary measures due to the foundation it sets if an attack occurs.

**Reasons for penetration testing**

-Establishing the likelihood of attacks

-Detecting high risk vulnerabilities resulting from low risk vulnerabilities

-Determining the bearing an attack will have.

Asessing the company’s network risk management capabilities

**Security measures for attacks**

-Craft strong passwords

-Enable two-step verification(Way of authenticating an individual’s identity using two components such as password,key, token,pin,biometrics)

-Be mindful of email attachment

-Regularly update software patches

-Question legitimacy of websites

-Keep updating anti-malware and anti-virus software

**Mobile phone Protection**

-Use token and encrypt on sensitive data

-Place Lock on Phone

-Don’t save passwords.

**Social Network Security**

-Don’t reveal location

-Keep birthday hidden

-Have private profile

-Don’t link accounts

**Prevention Software**

-Firewalls

-Virtual Private Network

-Anti-Virus and Anti-Spyware software

-Routine updates

**Critical cyber threats**

* Cyberterrorism
* Cyberwarfare – war against another country to damage its information networks
* Cyberespionage – Aim is to obtain the secerts of another without permission

**Defense of Hackers.**

Cryptograpy – secret method of writing

Examples of encryption methods:

International Data Encryption Method(IDEA)

Advanced Encryption Standard(AES)

Data Encryption Standard(DES)

**Digital Forensics**

-Sitautions where law enforcement collects and analyses data that can used in court against the perpetrator.

**Intrusion Detection Systems(IDSs)**

-Systems designed to report unauthorized people or programs on the network.

**Factors to consider before purchase of an IDS**

* Main purpose of the IDS
* Affordability
* Compatibility
* What happens if the IDS get a problem

**Examples of IDS manufacturers:**

* Dakota Alert Inc.
* Juniper Networks
* Linear LLC
* PureTech Systems Inc.
* Telguard

**Important information to take note**

* You can prevent or lessen the effect of cyberattacks by crafting strong passwords, using two-step verification, being careful while downloading attachments, and taking precautionary measures when you visit websites.
* You can protect your mobile phone by avoiding saving sensitive or financial data on your mobile phone or safeguarding your data by using specific methods such as tokenization and/or encryption; locking your phone when not in use; avoiding saving passwords, and avoiding saving personalized contacts list.
* You can protect your social network accounts by avoiding revealing your location, keeping your birthdate hidden, and avoiding linking your social accounts.
* You can avoid or lessen exposure to cyber threats by using security software such as firewalls, Virtual Private Networks (VPNs), antivirus, and antispyware. You also need to update them regularly.
* Critical cyber threats are those actions that, if carried out, may have a debilitating effect on organizations or even countries.
* Critical cyber threats can have different types, such as cyber terrorism, cyber warfare, and cyber espionage.
* You can utilize and understand effective security methods such as cryptography, digital forensics, intrusion detection, and legal recourses.