**Chapter 0**

* Security Terms:
  + Information Security : Processes and policies designed to protect ns organization’s info and info systems from unauthorized access, use, se, disclosure, disruption, modification, or destruction
  + Vulnerability is the flaw in the environment that someone can attack and harm the organization
  + Threat to an info resource is any danger to which a system may be exposed
  + Exposure of an info resources is the harm, loss or damage that can result if a threat comprises that resource.
    - Vulnerability : A crack on window
    - Threat : Severe weather outside
    - Exposure : A heavy rain going through the crack and damaging inside
* Five Factors Increasing The Vulnerability Of Information Resources
  + Today’s interconnected, interdependent, wirelessly-networked business environment
  + Smaller, faster, cheaper computers and storage devices
  + Decreasing skills necessary to be a hacker
  + Organized crime taking over cybercrime
  + Lack of management support
* Strong passwords
* Passwords are difficult to break
* Passwords should optimally have at least 15 characters
* Passwords should be a random combination of letters, numbers, and special characters
* Passwords should be replaced with new passwords at least every 60 days
* Passwords should not be reused for 12 months
* The same password should not be duplicated and used for multiple account
* Cyber-terrorism Vs. Cyber-warfare
  + Cyber-terrorism would be something done by a group of hackers done to inflict fear upon the victims (i.e.: stealing thousands of credit card #s to influence the actions of a major banking corporation).
  + Cyber-warfare would be the actions done by a nation or army to damage or defect the ability or other things of another country (i.e.: disabling the defense of the pentagon in order to stall military action of the USA in a war).
* Deliberate Threats
  + Competitive intelligence consists of legal information-gathering techniques
  + Industrial espionage crosses the legal boundary
  + Information extortion
    - Extortion is a criminal offense of obtaining money, property, or services from an individual or institution, through coercion
* Deliberate Acts
  + Spyware collects personal information about users without their consent. Two types of spyware are keystroke loggers (keyloggers) and screen scrapers.
  + Keystroke loggers record your keystrokes and your Web browsing history
  + Screen scrapers record a continuous “movie” of what you do on a screen.
* Software Attacks
  + A virus is a segment of computer code that performs malicious actions by attaching to another computer program.
  + A worm is a segment of computer code that spreads by itself and performs malicious actions without requiring another computer program.
* Deliberate Threats
  + A Trojan horse is a software program that hides in other computer programs and reveal its designed behavior only when it is activated.
  + A logic bomb is a segment of computer code that is embedded within an organization’s existing computer programs and is designed to activate and perform a destructive action at a certain time and date.
  + Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
* Compromises to intellectual property
  + Intellectual property. Property created by individuals or corporations which is protected under trade secret, patent, and copyright laws.
  + Intellectual property rights : Ownership and use of intellectual property such as software, music, movies, data, and information
  + Trade secret. Intellectual work, such as a business plan, that is a company secret and is not based on public information.
  + Patent. Document that grants the holder exclusive rights on an invention or process for 20 years.
  + Copyright. Statutory grant that provides creators of intellectual property with ownership of the property for life of the creator plus 70 years.
  + Piracy. Copying a software program without making payment to the owner.
* Graphical user interface, text

  Description automatically generated
* Authorization - Permission issued to individuals and groups to do certain activities with information resources, based on verified identity.
* Safelisting is a process in which a company identifies the software that it will allow to run and does not try to recognize malware.
* Blocklisting is a process in which a company allows all software to run unless it is on the blocklist.
* Encryption. Process of converting an original message into a form that cannot be read by anyone except the intended receiver.
* Firewalls. System that enforces access-control policy between two networks
* Anti-malware systems (also called antivirus software) are software packages that attempt to identify and eliminate viruses, worms, and other malicious software. The logos show three well-known anti-malware companies. Clicking on the link will take you to each company’s homepage, respectively
* Physical controls. Physical protection of computer facilities and resources.
* Access controls. Restriction of unauthorized user access to computer resources; use biometrics and passwords controls for user identification
* Communications (network) controls. To protect the movement of data across networks and include border security controls, authentication and authorization.
* Information systems auditing. Independent or unbiased observers task to ensure that information systems work properly.
* Audit. Examination of information systems, their inputs, outputs and processing.
* Auditing around the computer means verifying processing by checking for known outputs or specific inputs.
* Auditing through the computer means inputs, outputs and processing are checked.
* Auditing with the computer means using a combination of client data, auditor software, and client and auditor hardware