Reviewer CS 423

Chapt1

Ethics - is a code of behavior that is defined by the group to which an individual belongs.

Ethical Behavior - conforms to generally accepted norms, which may change over time to meet the evolving needs of the society or a group of people who share similar laws, traditions, and values that provide structure to enable them to live in an organized manner.

Morals - are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong.

Virtue - is a habit that inclines people to do what is acceptable, and a vice is a habit of unacceptable behavior.

Corporate Social Responsibility - is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers

Supply Chain Sustainability - is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs

Stakeholder - is someone who stands to gain or lose, depending on how a particular situation is resolved.

Corporate Ethics Officer - (also called a corporate compliance officer) provides an organization with vision and leadership in the area of business conduct.

Code of Ethics - is a statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision-making.

Integrity - A person who acts with integrity acts in accordance with a personal code of principles

Chapt2

Relationship between IT workers and employers - IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT worker and an employer typically agree on the fundamental aspects of this relationship before the worker accepts an employment offer

Bribery - y is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.

Internal Control - I is the process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations

Policies - are the guidelines and standards by which the organization must abide.

IT User - refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product.

Whistleblowing - is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.

Fraud - is the crime of obtaining goods, services, or property through deception or trickery.

Misrepresentation - is the misstatement or incomplete statement of a material fact.

Breach of Contract - occurs when one party fails to meet the terms of a contract.

Trade Secret - is information, generally unknown to the public, that a company has taken strong measures to keep confidential.

Chapt3

Zero-day Exploit - is a cyberattack that takes place before the security community and/or software developers become aware of and fix a security vulnerability.

Exploit - is an attack on an information system that takes advantage of a particular system vulnerability

Chapt4

Data Privacy Act of 2012 (Purpose, Scope, Penalties)

Information Privacy - the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and their use).

Fair Information - is a term for a set of guidelines that govern the collection and use of personal data.

Chapt5

Freedom of Expression - is one of the most important rights for free people everywhere.

Internet Filter - is software that can be used to block access to certain websites that contain material deemed inappropriate or offensive.

Internet Censorship - is the control or suppression of the publishing or accessing of information on the Internet

Anonymous Expression - is the expression of opinions by people who do not reveal their identity. The freedom to express an opinion without fear of reprisal is an important right of a democratic society

Pornography on the Internet - Many people, including some free-speech advocates, believe that there is nothing illegal or

wrong about purchasing adult pornographic material made by and for consenting adults.

KEY TERMS:

-Type of Exploit (Worm, Trojan Horse, DDoS, RootKit) - There are numerous types of computer attacks, with new varieties being invented all the time. This section discusses some of the more common attacks, including ransomware, viruses, worms, Trojan horses, blended threats, spam, distributed denial-of service (DDoS) attacks, rootkits, advanced persistent threats, phishing and spear phishing, smishing and vishing, cyberespionage, and cyberterrorism.

a ***worm*** is a harmful program that resides in the active memory of the computer and duplicates itself

A ***Trojan*** horse is a seemingly harmless program in which malicious code is hidden

A ***distributed denial-of-service (DDoS)*** attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.

A ***rootkit*** is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge

-Advanced Persistence Threat - (APT) is a network attack in which an intruder gains access to a network and stays there—undetected—with the intention of stealing data over a long period of time (weeks or even months)

-***CyberTerrorism*** - is the intimidation of government or civilian population by using information technology to disable critical national infrastructure (for example, energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals

-***Phishing*** - is the act of fraudulently using email to try to get the recipient to reveal personal data

-***Spear Phishing*** - is a variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees. It is known as spear phishing because the attack is much more precise and narrow, like the tip of a spear.

-***Vishing*** - is similar to smishing except that the victims receive a voice-mail message telling them to call a phone number or access a website

-***Smishing*** - is the act of fraudulently using email to try to get the recipient to reveal personal data

-***Email Spam*** - is the use of email systems to send unsolicited email to large numbers of people

-***Cyber Attack -*** any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device

-***Ransomware*** - is malware that stops you from using your computer or accessing your data until you meet certain demands, such as paying a ransom or sending photos to the attacker

-***Virus*** - is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.

-***Router*** - is a networking device that connects multiple networks together and forwards data packets from one network to another

-***Consumer Profiling*** - Companies openly collect personal information about users when they register at websites, complete surveys, fill out forms, follow them on social media, or enter contests online.

-***Electronic Surveillance*** - This section discusses government surveillance, including various forms of electronic surveillance, as well as some of the laws governing those activities

-***Camera Surveillance*** - Surveillance cameras are used in major cities around the world in an effort to deter crime and terrorist activities

-***Vehicle Event Data Reporters*** - a device that records video in a vehicle to create a record of accidents and for evaluating driver and vehicle performance.

-***Stalking Apps/Application -*** phones to secretly track or monitor you.