Ethical Frameworks

1. Utilitarian Approach - most good or least harm
2. Rights Approach - best protects and respects the moral rights of the affected parties.
3. Fairness Approach - treat all human beings equally, or, if unequally, then fairly, based on some defensible standard.
4. Common Good Approach - respect and compassion for all others is the basis for ethical actions.

Five Steps of the General Ethical Framework

1. Recognize the Issue
2. Get the facts
3. Evaluate Alternative Actions
4. Make a Decision and Test It
5. Act and Reflect on the Outcome of Your Decision

Fundamental Tenets of Ethics

1. Responsibility:means that you accept the consequences of your decisions and actions
2. Accountability:refers to determining who is responsible for actions that were taken.
3. Liability:a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

Ethical Issues:

1. Privacy Issues : involve collecting, storing, and disseminating information about individuals.
2. Accuracy Issues: involve the authenticity, fidelity, and correctness of information that is collected and processed.
3. Property Issues:involve the ownership and value of information.
4. Accessibility Issues:revolve around who should have access to information and whether they should pay a fee for this access.

PRIVACY

Two rules

1. The right to privacy is not absolute
2. The public’s right to know supersedes the individual’s right to privacy.

Electronic Surveillance

Personal Information in Databases

* How are the data used?
* To whom are the data given or sold?
* How secure are the data against access by unauthorized people?

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

Principles of Information Security

* Confidentiality
* Integrity
* Availability
* Non-repudiation
* Authenticity
* Accountability

Causes

* Failures
* Human actions
* Natural Disasters

Security threats control measures

* Develop a security plan
* Secure IT Infrastructure
* Use stronger passwords
* Know and protect important information
* Manage file access permissions
* Regularly backup data
* Regular data audits
* Staff awareness

Privacy Codes and Policies

* Privacy policies
* Opt-Out Model of Informed Consent
* Opt-In Model of Informed Consent
* Platform for Privacy Preferences (P3P)

International Aspects of Privacy

* Inconsistent Privacy and Security Laws
* Transborder data flow
* European Community Commission
* Safe Harbor framework for European citizen personal data

Five factors increasing security vulnerabilities

1. Today’s interconnected, interdependent, wirelessly networked business environment
2. Smaller, faster, cheaper computers and storage devices
3. Decreasing skills necessary to be a computer hacker
4. International organized crime taking over cybercrime
5. Lack of management support

Unintentional threats to IS:

1. Human Errors
2. Social engineering

* Phishing
* Tailgating
* Baiting
* Pretexting

Deliberate threats to IS:

1. Espionage or Trespass
2. Information Extortion
3. Sabotage or Vandalism
4. Theft of Equipment or Information
5. Identity Theft
6. Compromises to Intellectual Property
7. Software Attacks
8. Alien Software
9. Supervisory Control and Data Acquisition Attacks(SCADA)
10. Cyberterrorism and Cyberwarfare

Compromises to Intellectual Property

* Intellectual Property
* Trade Secret
* Patent
* Copyright

Software Attacks

1. Remote Attacks Requiring User

* Action
* Virus
* Worm
* Phishing Attack
* Spear Phishing

1. Remote Attacks Needing No User Action

* Denial-of-Service Attack
* Distributed Denial-of-Service Attack

1. Attacks by a Programmer Developing a System

* Trojan Horse
* Back Door
* Logic bomb

Alien Software

* Adware
* Spyware

1. Keystroke loggers
2. Screen scrapers

* Spamware
* Cookies

What organizations are doing to protect information

1. Risk
2. Risk Management
3. Risk analysis
4. Risk mitigation
5. Controls evaluation
6. Risk Analysis

Three Steps of Risk Analysis

1. assessing the value of each asset being protected
2. estimating the probability that each asset will be compromised
3. comparing the probable costs of the asset’s being compromised with the costs of protecting that asset
4. Risk Mitigation

risk mitigation strategies that organizations can adopt

1. Risk Acceptance : Accept the potential risk, continue operating with no controls, and absorb any damages that occur
2. Rick Limitation : Limit the risk by implementing controls that minimize the impact of the threat.
3. Risk Transference : Transfer the risk by using other means to compensate for the loss, such as by purchasing insurance

INFORMATION SECURITY CONTROLS

1. Physical Controls
2. Access Controls

* Authentication
* Authorization

1. Communications Controls

Firewall, Anti-malware Systems, Whitelisting, Blacklisting, Encryption, Virtual Private Network (VPN), secure socket layer (SSL), employee monitoring systems

1. Business Continuity Planning
2. Information Systems Auditing

Three categories

1. Auditing Around the Computer
2. Auditing Through the Computer
3. Auditing With the Computer