Ethical Issues & Privacy

….It easier to store and transfer personal information

…Threats to privacy

…Protect the buyers' identities

…Privacy issue is tracking ect the buyers' identities

…Cookies

..Antivirus software

..Harmful cookies

Ethics

- Ethics
  - A branch of philosophy that deals with what is considered to be right and wrong.
- A Code of Ethics
  - A code of ethics is a collection of principles intended as a guide for members of a company or organization.

Ethical Terminology

- Responsibility
  - means that you accept the consequences of your decisions and actions.
- Accountability
  - means a determination of who is responsible for actions that were taken.
- Liability
  - a legal concept meaning that individuals have the right to recover the damages done to them by other individuals, organizations, or systems.

Ethical Issues

- The diversity and ever expanding use of IT applications have created a variety of ethical issues.
- These issues fall into four general categories:
  - 1. Privacy issues involve collecting, storing, and disseminating information about individuals.
  - 2. Accuracy issues involve the authenticity, fidelity, and accuracy 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 have to pay for this access.

Computer Crime

Definition: the act of using a computer to commit an illegal act

- Authorized and unauthorized computer access
- Examples
  - Stealing time on company computers
  - Breaking into government Web sites
  - Stealing credit card information

Computer Crime

Federal and State Laws

- Stealing or compromising data
- Gaining unauthorized computer access
- Violating data belonging to banks
- Intercepting communications
- Threatening to damage computer systems
- Disseminating viruses

Hacking and Cracking

- Hacker – one who gains unauthorized computer access, but without doing damage
- Cracker – one who breaks into computer systems for the purpose of doing damage

Information System Ethics

Computer viruses and destructive code

- Virus – a destructive program that disrupts the normal functioning of computer systems
- Types:
  - Worm: usually does not destroy files; copies itself
  - Trojan horses: Activates without being detected; does not copy itself
  - Logic or time bombs: A type of Trojan horse that stays dormant for a period of time before activating

Computer Security

Computer Security – precautions taken to keep computers and the information they contain safe from unauthorized access

Recommended Safeguards

- Implement a security plan to prevent break-ins
- Have a plan if break-ins do occur
- Make backups!
- Only allow access to key employees
- Change passwords frequently
- Keep stored information secure
- Use antivirus software
- Use biometrics for access to computing resources
- Hire trustworthy employees

Computer Security

Encryption – the process of encoding messages before they enter the network or airwaves, then decoding them at the receiving end of the transfer

Ethical Issues &Privacy

- The use of information systems and technology impacts individuals, groups, and societies. Technology must be used ethically and designed to avoid injuring humans.

Ethical Issues

- Policies and procedures must be established to avoid computer waste and mistakes.
- Although often unintentional, computer waste and mistakes can be costly. Organizational policies & procedures can help avoid losses.
- Intentional computer crime is rapidly increasing and requires the attention of management and security specialists.

Computer Waste

- Discard technology
- Unused systems
- Personal use of corporate time and technology

Computer Waste

- Computer waste is widespread in the public and private sectors, and is usually caused by the improper management of information technology.
- Some companies discard usable hardware and software that could be used elsewhere in the company, or sold or donated.
- Another example of computer waste occurs when significant resources are invested in the development of an information system, and then, it is never used to it fullest extent.
- This happens for many reasons, but poor design and inadequate training are major causes. Employees playing computer games or surfing the Web at their desks during working time is also a source of waste, as are junk e-mail and junk faxes.

Preventing Computer Waste and Mistakes

- Establish Policies and Procedures
- Implement Policies and Procedures
- Monitor Policies and Procedures
- Review Policies and Procedures
- Procedures relating to the acquisition and use of computers can avoid both waste and mistakes. For example, procedures could ensure that computers no longer needed in one part of the company would be used in another part, rather than discarded.

Preventing Computer Waste and Mistakes

- Employees and groups are less likely to make mistakes using applications and technology if they have been properly trained in their use.
- Many organizations require that systems or applications meeting certain criteria must be approved by a committee or the IS department before they are acquired or implemented, to ensure they are compatible with existing systems, databases, and technology, and are cost-effective.
- Many organizations have established procedures to ensure that all systems, including those developed by end users, have adequate documentation.

Why to secure information

- Recognize that organizations have a business need for information security
- Understand that a successful information security program is the responsibility of both an organization's general management and IT management
- Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems from attacks against the information within systems

Information Security

- Primary mission of information security is to ensure systems and contents stay the same
- If no threats, could focus on improving systems, resulting in vast improvements in ease of use and usefulness
- Attacks on information systems are a daily occurrence

What Business Needs

- Information security performs four important functions for an organization
  - Protects ability to function
  - Enables safe operation of applications implemented on its IT systems
  - Protects data the organization collects and uses
  - Safeguards technology assets in use
  - Organization should address information security in terms of business impact and cost

Threats

- Threat: an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the different threats facing the organization
- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

Categories of Threats

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

What is Information Security?

- Typical definition: *The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*
- Security is a non-functional requirement - Assumes that the system is correctly implemented according to the functional requirements of its specification
- Ensures that the system operates according to its intention
- Security is a process not a product
  - Concerns the specification of the system
  - Concerns the design and implementation of the system *Application code and protocols*
  - Concerns the installation and operation of the system *Configuration and operation parameters*
  - *Human factors (users and administrators)*

Information is an Asset

- Security is against the confidentiality of the data, integrity of data/information availability of the data

Information Asset

- INFORMATION ASSET" as defined in section 2(f) of the Information Technology Act 2000 -
- All Information resources utilized in the course of any organization's business
  - includes all information, applications (Software developed or Purchased) & Technology (Hardware, System Software &

What is information

- Information is the lifeblood of modern civilization.
  - In the form of data it is the raw material from which understanding and, ultimately, controls are fashioned.
  - Compiled, analyzed, considered and reported, it is an asset and a currency of exchange.
  - As ideas and concepts it is the intellectual capital that shores up our economic system and our way of life.
- Information can be stored, moved easily and cheaply from place to place, and replicated ad infinitum.

What is Information

- It is a form of knowledge that we acquire through education, communication, practical experience, research, analysis.
- It consists of data, facts, and conclusions.
- To the engineer it is any data that can be expressed as a sequence of ones and zeros.

Five key factors increasing vulnarability

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

Two main Types of threats

- Unintentional
- Intentional

Unintentional

- Carelessness with computing device
- Opening questionable emails
- Carless Internet surfing
- Poor password strength
- Carelessness in the office

Intentional

- Espionage, trespass, extortion
- Theft of equipment or information
- Identity theft
- Software attacks

Information Can be

- Created
- Modified
- Stored
- Destroyed
- Processed
- **Used – (For proper & improper purposes)**
- Transmitted
- Corrupted
- Lost
- Stolen

Information can be

- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronics means
- Shown on corporate videos
- Displayed / published on web
- Verbal – spoken in conversations

Critical Characteristics of Information

The value of information comes from the characteristics it possesses.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility

Controlling Information System

- There are numerous threats to Information Systems
  - Hardware failures
  - Software failures
  - Upgrade issues
  - Disasters
  - Malicious intent

Controlling Information System

- Implemented through
  - Policies
  - Procedures
  - Standards
- Control must be thought about through all stages of Information Systems analysis, construction, deployment operations and maintenance

Controls

- General controls
  - Controls for design, security and use of Information Systems throughout the organisation
- Application controls
  - Specific controls for each application
  - User functionality specific

General Controls

- Implementation controls
  - Audit system development
  - Ensure properly managed and controlled
  - Ensure user involvement
  - Ensure procedures and standards are in use
- Software controls
  - Authorised access to systems

General Controls

- Hardware controls
  - Physically secure hardware
  - Monitor for and fix malfunction
  - Environmental systems and protection
  - Backup of disk-based data

General Controls

- Computer operations controls
  - Day-to-day operations of Information Systems
  - Procedures
  - System set-up
  - Job processing
  - Backup and recovery procedures

General Controls

- Data security controls
  - Prevent unauthorised access, change or destruction
  - When data is in use or being stored
  - Physical access to terminals
  - Password protection
  - Data level access controls

General Controls

- Administrative controls
  - Ensure organisational policies, procedures and standards and enforced
  - Segregation of functions to reduce errors and fraud
  - Supervision of personal to ensure policies and procedures are being adhered

Application Controls

- Input controls
  - Data is accurate and consistent on entry
  - Direct keying of data, double entry or automated input
  - Data conversion, editing and error handling
  - Field validation on entry
  - Input authorisation and auditing
  - Checks on totals to catch errors

Application Controls

- Processing controls
  - Data is accurate and complete on processing
  - Checks on totals to catch errors
  - Compare to master records to catch errors
  - Field validation on update

Application Controls

- Output controls
  - Data is accurate, complete and properly distributed on output
  - Checks on totals to catch errors
  - Review processing logs
  - Track recipients of data

Protecting Your Privacy

- Use strong passwords
- Adjust privacy settings on your computer
- Surf the Web anonymously
- E-mail anonymously
- Erase your Google search history

Protecting Information Systems

- Information Systems, especially TPS, require high degrees of availability
- Technology is available to ensure systems are available and contain accurate information

Information Security

- The application of technology and processes to protect data from accidental or intentional misuse persons known or unknown inside or outside of an organization.
- By no means strictly a technical aspect, its technical aspects (firewalls, encryption, access controls, etc.) are important, but so are processes applied to ever varying situations.
- An increasingly high-profile problem as hackers (or crackers) take advantage of vulnerabilities against parts of an organization's network either Internet accessible or internal.