CYBER LAW AND POLICY

Chapter One

Legal and ethical issues in computer security

Introduction

- You must understand scope of an organization's legal and ethical responsibilities
- To minimize liabilities/reduce risks, the information security practitioner must:
  - Understand current legal environment
  - Stay current with laws and regulations
  - Watch for new issues that emerge

Law and Ethics in Information Security

- Law is a legal system comprising of rules and principles that govern the affairs of a community and controlled by a political authority
- ethics in computing means proper guidelines to refer to when using the computer and computer networks. This includes the Internet.
- Ethics: define socially acceptable behavior

Organizational Liability and the Need for Guidance

- Liability: legal obligation of an entity extending beyond criminal or contract law; includes legal obligation to make restitution
- Restitution: to compensate for wrongs committed by an organization or its employees
- Due care: insuring that employees know what constitutes acceptable behavior and know the consequences of illegal or unethical actions

Law vs. ethics

- **Law:** is a legal system comprising of rules and principles that govern the affairs of a community and controlled by a political authority

- **Ethics:** in computing means proper guidelines to refer to when using the computer and computer networks. This includes the Internet.

Law & ethics

- **WHY DO WE NEED ETHICS AND LAW IN COMPUTING?**

1. Respecting Ownership
2. Respecting Privacy & secrecy
3. Respecting Property

Law & ethics

1. RESPECTING OWNERSHIP

- We must respect ownership by not stealing other people's work either by duplicating or distributing it. Duplicating and distributing copies of audio tapes, video tapes and computer programs without permission and authorization from the individual or company that created the program are immoral and illegal.

2. RESPECTING PRIVACY AND CONFIDENTIALITY

- We should respect other people's privacy and confidentiality by refraining ourselves from reading their mails or files without their permission. If we do so, it is considered as violating an individual's rights to privacy and confidentiality.

3. RESPECTING PROPERTY:

Since an individual data and information are considered as property, therefore, an act of tampering and changing electronic information is considered as vandalism and disrespect for other people's property.

Ethics and Information Security

The Ten Commandments of Computer Ethics [6]

From The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical
- Difficulties arise when one nationality's ethical behavior conflicts with ethics of another national group
- **Example**: many of the ways in which Asian cultures use computer technology is considered software piracy by other nations

Restriction of Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior: **ignorance, accident, intent**
- Deterrence: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls
- Laws, policies, and controls only deter if two conditions are present:
  1. Fear of penalty
  2. Probability of being caught

Similarities between Law and Ethics

Both ethics and law are complimentary to each other and are made:

- to guide user from misusing computers
- to create a healthy computer society, so that computers are used to contribute to a better life
- to prevent any crime

Difference between Law and Ethics

ETHICS:

GUIDELINE As a guideline to computer users.

MORAL STANDARDS Ethical behaviour is judged by moral standards.

FREE TO FOLLOW Computer users are free to follow or ignore the code of ethics.

NO PUNISHMENTS No punishment for anyone who violates ethics.

UNIVERSALS Universal, can be applied anywhere, all over the world.

PRODUCE ETHICAL COMPUTER USERS To produce ethical computer users.

Differences between Law and Ethics

- **LAW:**

  CONTROL As a rule to control computer users.

  JUDICIAL STANDARDS Law is judged by judicial standards.

  MUST FOLLOW Computer users must follow the regulations and law.

- **PENALTIES, IMPRISONMENTS AND OTHER PUNISHMENTS : Penalties, imprisonments and other punishments for those who break the law.**

- **DEPENDS ON COUNTRY Depends on country and state where the crime is committed.**

Policy versus Law

- **Policies:** body of expectations that describe acceptable and unacceptable employee behaviors in the workplace
- Policies function as laws within an organization; must be crafted carefully to ensure they are complete, appropriate, fairly applied to everyone
- Difference between policy and law: ignorance of a policy is an acceptable defense
- Criteria for policy enforcement: dissemination (distribution), review (reading), comprehension (understanding), compliance (agreement), uniform enforcement(implementation)

What is cyber crime

- Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Why computer crime is hard to define

1. Understanding : neither courts, lawyer, nor police agent necessary understands computers

2. Tangible evidence : police and courts fro years depends on tangible evidence like fingerprints

3. Form of assets: we know what cash is , but are 20 invisible magnetic spots equal million of dollars