Information Security and Network Security

Chapter – 1

Introduction to Information Security

Legal, Ethical & Professional Issues in Information Security

1. Ethical Issues

Information systems have made many businesses successful today. Improper use of information techno's can create problems for organization and employees. e.g. Criminals gaining access to credit card information can lead to financial loss to the owners of the ears or financial Institute.

- Using Organization Information system i.e. posting inappropriate Content on face book or twitter using company account can lead to lawsuits (Claim or dispute brought to law court) and loss of business.

People as part of the information system components can also exploited using social engineering techniques. The goal of social engineering is to gain trust of the users of the system.

Information system ethics refers to rules of right and wrong that people use to make choices to guide their behaviors. Ethics in MIS seek to protect and safeguard individuals and society by using information systems responsibly.

- Most Profession affiliated with the profession must adhere to

- Code of ethics makes individuals acting on their free will responsible and accountable for their actions.

Ethics & Education

- what are expected behaviors of an ethical employees.

- To understand that their behavior is unethical or even illegal.

- Proper ethical and legal training is vital.

Ethical issues in security include to respect human rights. the importance of transparency and accountability and responsibility to protect the confidentiality of information. Legal, Ethical &Professional Issues in Information satiny.

2. Legal Issues.

Legal issues in information security similar to ethical issues, Information Technology Organizations are also bound to follow laws issued by the government

- If company fails to provide satisfactory service to the client or cheats the client, the organization in held guilty in court.

- Laws are rules that mandate or prohibit certain behavior in society, they are drawn from ethics, which define socially acceptable behaviors.

1) National Information Infrastructures Protection Act 1996 – Crimes based, on defendants authority to access computer and carinal intent.

2) Privacy of Costumer Information - federal friary act 1974 - Governs Federal agency use of Personal information.

3) The electronic Communication Privacy act of 1986 – cryptography - Security and freedom through Encryption Act of 1999 – use and sale of S/W that uses or enables encryption.

4) Computer fraud and abuse Act-1986 - Defines and formalize laws to counter threats from computer related acts and offenses.

5) Computer Security act 1987 - Requires all Federal Computer systems that contain classified information have security plans in place and requires periodic security training for all individuals who operate, design or manage such system.

In addition to above

- State & local regulations

- International Laws & Legal bodies

3) Professional Issues

Security Professional play a critical role in protecting organizations from security threats both Internal and external. They must adhere to legal and ethical standards while performing the duties. To ensnare that they do not violate the rights of individuals or infringe on their privacy.

Security professionals must possess the necessary qualification and certifications to work in the Industry, engage in ongoing, professional development, and undergo regular training to stay up-to–date with the latest security threats and best practices.

They must also comply with data protection laws, respect the privacy and human rights of individuals and protect the confidentiality of individuals, and protect the Confidentiality of Information.

By adhering (believe in and follow the practice) to their professional standards. Security professional can provide the best possible security services to their clients and protect them from security threats.

Some issues as:

1) Qualification and Certifications. Common certifications include
   - Certified Information Systems Security Professionals (CISSP)
   - Certified Ethical Hackler (CEH)
   - Certified Information security Manager (CISM) &
   - Certified Information Systems Auditor (CISA)

Shon of manpower possessing certification.

2) Professional Development:

Must engage in ongoing professional development to spray up-to-date with the latest security trends, technology, and best practices

This can Include:

- Attending Conferences
- Taking online Courses & participating in an industry event.

On Professionals must undergo ongoing training to ensure that they are aware at the latest security threats and how to respond to them.

This can in Cloned training on -

- Physical security

- Cyber security

- Erogeneity response procedures

By undergoing eternal training security professionals can ensure that they are prepared to respond to any security threat that may arise.