1.1 LEGAL, ETHICAL AND PROFESSIONAL ASPECTS OF SECURITY

Today millions of people perform online transactions every day. There many ways to attack computer and networks to take advantage of what has made shopping, banking, transformation of messages, investments and leisure pursuits a simple matter of dragging and clicking for many people. Thus, the laws and ethics are important aspects in data and network security. The legal system has adapted quite well to computer technology by reusing some old forms of legal protection (copyrights and patents) and creating laws where no adequate one existed (malicious access). Still the courts are not a perfect form of protection for computer, for two reasons, first court tends to be reactive instead of proactive. That is, we have to wait for regression to occur and then adjudicative it, rather than try to prevent it in first place. Second fixing a problem through the courts can be time consuming and more expensive.

The latter characteristic prevents all but the wealthy from addressing most wealthy. On other hand, 1ethics has not had to change , because ethic is more situational and personal than the law, for example the privacy of personal information becoming important part of computer network security and although technically this issue is just an aspect of confidentiality, practically it has a long history in both law and ethics.

Law and security are related in several ways. First international, national, state, city laws affect privacy, secrecy. These statutes often apply to the rights of individuals to keep personal matters private. Second law regulates the use of development, and ownership of data and programs. Patents, copy rights, and trade secrets are legal devices to protect the right of developers and owners of the information and data.

1.1.1 Cryptography and Law

Cyber-Crime: - Criminal activities or attacks in which computer and computer networks are tool, target, or place of criminal activity. Cybercrime categorize based on computer roles such as target, storage device and communication tool.

Computers as targets: To get the information from the computer system or control the computer system without the authorization or payment or alter the interfaces or data in the particular system with use of server.

Computers as storage devices: Computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen password lists, credit card details and proprietary corporate information.

Computers as communications tools: Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. Other than these crimes there are more specific crimes in computer networks. There are:

Illegal access: The access to the whole or any part of a computer system without right. Illegal interception: The interception without right, made by technical means, of non-publictransmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Data interference: The damaging, deletion, deterioration, alteration or suppression of computer

data without right.

System interference: The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Computer-related forgery: The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Crime related to child pornography: Producing child pornography or distribution through a computer system and making available or distributing or transmitting child pornography through a computer system.

The relative lack of success in bringing cyber-criminals to justice has led to an increase in their numbers, boldness, and the global scale of their operations. It is difficult to profile cybercriminals in the way that is often done with other types of repeat offenders. The success of cybercriminals and the relative lack of success of law enforcement, influence the behaviour of cybercrime victims. As with law enforcement, many organizations that may be the target of attack have not invested sufficiently in technical, physical, and human-factor resources to prevent attacks.

The law is used regulate people for their own good and for the greater good of society. Cryptography also regulated activity.

Some Example laws which are forced on cryptography.

Control use of cryptography: Closely related to restrictions on content are restrictions on the use of cryptography imposed on users in certain countries. For examples, 2 In China, state council order 273 requires foreign organizations or individuals to apply permission to use encryption in China. Pakistan requires that all encryption hardware and software be inspected and approved by the Pakistan telecommunication authority.

Cryptography and Free speech: The Cryptography involve not just products, it involves ideas too, although governments effectively control the flow of products across borders, controlling the floe ideas either head or on the internet, is also impossible.

Cryptography and Escrow: Although laws enable governments to read encrypted communications. In 1996, US government offered to relax the export restriction for so called escrowed encryption, in which the government would able to obtain the encryption key for any encrypted communication.

The victory in use of law enforcement depends much more on technical skills of the people. Management needs to understand the criminal investigation process, the inputs thatinvestigators need, and the ways in which the victim can contribute positively to the investigation.

1.1.2 Intellectual Properties.

There are three main types of intellectual property for which legal protection is available. **Copy rights:** Copyright law protects the tangible or fixed expression of an idea, not the idea itself. Copy right properties exists when proposed work is original and creator has put original idea in concrete

form and the copyright owner has these exclusive rights, protected against infringement such as reproduction right, modification right, distribution right

Patents: A patent for an invention is the grant of a property right to the inventor. There are 3 types in patents:-

- Utility (any new and useful process, machine, article of manufacture, or composition of matter).
- Design (new, original, and ornamental design for an article of manufacture)
- Plant (discovers and asexually reproduces any distinct and new variety of plant).

Trade-Marks: A trademark is a word, name, symbol or expression which used to identify the products or services in trade uniquely from others. Trade mark rights used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark.

- Intellectual Property Relevant to Network and Computer Security A number of forms of intellectual property are relevant in the context of network and computer security.
- Software programs: software programs are protected by using copyright, perhaps patent.
- Digital content: audio / video / media / web protected by copy right Algorithms: algorithms may be able to protect by patenting
- Privacy Law and Regulation: An issue with considerable overlap with computer security is that of privacy. Concerns about the extent to which personal privacy has been and may be compromised have led to a variety of legal and technical approaches to reinforcing privacy rights. A number of international organizations and national governments have introduced laws and regulations intended to protect individual privacy.
- European Union Data Protection Directive was adopted in 1998 to ensure member states protect fundamental privacy rights when processing personal info and prevent member states from restricting the free flow of personal info within EU organized around principles of notice, consent, consistency, access, security, onward transfer and enforcement. US Privacy Law have Privacy Act of 1974 which permits individuals to determine records kept, forbid records being used for other purposes, obtain access to records, ensures agencies properly collect, maintain, and use personal info and createsa private right of action for individuals.Cryptography and Ethics.

- There are many potential misuses and abuses of information and electronic communication that create privacy and security problems. Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions. An ethic an objectively defined standard of right and wrong. Ethical standards are often idealistic principles because they focus on one objective. Even though religious group and professional organization promote certain standards of ethical behaviour, ultimately each person is responsible for deciding what do in a specific situation.

1.1.3 Ethical issues related to computer and info systems

Computers have become the primary repository of both personal information and negotiable assets, such as bank records, securities records, and other financial information.

Repositories and processors of information: Unauthorized use of otherwise unused computer services or of information stored in computers raises questions of appropriateness or fairness.

Producers of new forms and types of assets: For example, computer programs are entirely new types of assets, possibly not subject to the same concepts of ownership as other assets.

Symbols of intimidation and deception: The images of computers as thinking machines, absolute truth producers, infallible, subject to blame, and as anthropomorphic replacements of humans who err should be carefully considered.

1.2 NEED FOR SECURITY AT MULTIPLE LEVELS

Multilevel security or multiple levels of security (MLS) is the application of a computer system to process information with incompatible classifications (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.

There are two contexts for the use of multilevel security.

One is to refer to a system that is adequate to protect itself from subversion and has robust mechanisms to separate information domains, that is, trustworthy.

Another context is to refer to an application of a computer that will require the computer to be strong enough to protect itself from subversion and possess adequate mechanisms to separate information domains, that is, a system we must trust. This distinction is important because systems that need to be trusted are not necessarily trustworthy.

A threat is an object, person, or other entity that represents a constant danger to an asset.

1.2.1 Security Policies

The Cryptography Policy sets out when and how encryption should be used. It includes protection of sensitive information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

Role of the Security Policy in Setting up Protocols

Following are some pointers which help in setting u protocols for the security policy of an organization.

- Who should have access to the system?
- How it should be configured?
- How to communicate with third parties or systems?

Policies are divided in two categories:

- User policies
- IT policies.

User policies generally define the limit of the users towards the computer resources in a

workplace. For example, what are they allowed to install in their computer, if they can use removable storages?

Whereas, IT policies are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies** − This is the policy which defines the rights of the staff and access level to the systems. Generally, it is included even in the communication protocol as a preventive measure in case there are any disasters.
- **Server Policies** − This defines who should have access to the specific server and with what rights. Which software's should be installed, level of access to internet, how they should be updated?
- **Firewall Access and Configuration Policies** − It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound?
- **Backup Policies** − It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.
- **VPN Policies** − These policies generally go with the firewall policy; it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network, type of encryption to be set.

1.2.2 Structure of a Security Policy

When you compile a security policy you should have in mind a basic structure in order to make something practical. Some of the main points which have to be taken into consideration are:

- Description of the Policy and what is the usage for?
- Where this policy should be applied?
- Functions and responsibilities of the employees that are affected by this policy.
- Procedures that are involved in this policy.
- Consequences if the policy is not compatible with company standards.

Types of Policies

- **Permissive Policy** − It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploitsare taken in consideration.
- **Prudent Policy** − This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites is allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy** − This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.

- **User Account Policy** − This policy defines what a user should do in order to have or maintain another user in a specific system. For example, accessing an e-commerce webpage. To create this policy, you should answer some questions such as −
  - Should the password be complex or not?
  - What age should the users have?
  - Maximum allowed tries or fails to log in?
  - When the user should be deleted, activated, blocked?
- **Information Protection Policy** − This policy is to regulate access to information, hot to process information, how to store and how it should be transferred.
- **Remote Access Policy** − This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.
- **Firewall Management Policy** − This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.
- **Special Access Policy** − This policy is intended to keep people under control and monitor the special privileges in their systems and the purpose as to why they have it. These employees can be team leaders, managers, senior managers, system administrators, and such high designation based people.
- **Network Policy** − This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether that person should be authenticated or not. This policy also includes other aspects like, who will authorize the new devices that will be connected with network? The documentation of network changes. Web filters and the levels of access. Who should have wireless connection and the type of authentication, validity of connection session?
- **Email Usage Policy** − This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of this system that they have the privilege to use. They should not open any attachments that look suspicious. Private and confidential data should not be sent via any encrypted email.
- **Software Security Policy** − This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer. Warez and pirated software's should not be allowed.