Computer Misuse

Table Of Contents

Categories

- Computer Fraud
- Unauthorized obtaining of information from a computer
- Unauthorized alteration of information stored on a computer
- Denying access to an authorized user
- Unauthorized alteration or destruction of information stored on a computer
- Denying access to an authorized user
- Unauthorized removal of information stored on a computer

Computer Fraud

- Input Fraud
- Output Fraud
- Program Fraud

Unauthorized Obtaining Of Information

1. Computer Hacking
2. Eavesdropping on a computer
3. Making unauthorized use of computers for personal benefit

Under Section 1 of the Computer Misuse 1990, a person is guilty of an offence if,

1. He causes a computer to perform any function with intent to secure access to any program or data held on any computer

2. The access he intends to secure is authorized
3. He knows at the time when he causes te computer to perform the function that this is the case

Eavesdropping

Involves,

1. Secret listening
2. Secret watching

Unauthorized Altering Or Destruction Of Information

Computers store vast amounts of information about us,

1. What we have in the bank
2. Who we call on the telephone
3. What we buy in the shops
4. Where we travel

Criminals who alter or destroy such information can be dealt with by,

1. The law on Criminal Damage
2. The Computer Misuse Act 1990 section 3

Unauthorized Destruction Of Information

The law on Criminal Damage seems to apply to physically stored data for example,

1. Damage or delete data belonging to someone
2. Writing a program that damages the data on a hard disk

Reasons For Cyber Crime Not Being Reported

- Offences are difficult to prove
- Evidences are difficult to collect - firms usually do not cooperate with the police
- Firms are embarrassed or scared about their reputation due to hacking particularly banks
- Employees are normally sacked or demoted
- Police lack expertise; time; money
- The Cyber-Crime is perceived as ‘soft crime’, as no one gets physically injured or hurt

Current Situation

1. Hacking has increased with time
2. Few high profile cases

3. No equivalent legislation in other countries
4. Some 'international task forces' set up but no real progress

Cyber Laws In Pakistan

Two main,

- Electronic Transaction Ordinance 2002
- Electronic / Cyber Crime Bill 2007

Electronic Transaction Ordinance 2002

- Laid foundations for comprehensive Legal infrastructure
- Heavily taken from foreign law related to cyber crime

Cyber Crime Bill 2007

The bill deals with the electronic crimes including,

- Cyber Crime
- Data Damage: Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section
- Electronic Fraud: People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm
- Electronic Forgery: Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not
- Unauthorized Access To Code
- Cyber Stalking
- Cyber Spamming: Transmitting harmful, fraudulent, misleading

References

- Chapt 16 Computer Misuse