CHAPTER # 06

SECURITY, COPYRIGHT & THE LAW

COMPUTER CRIME:

Company crime is often defined as any crime accomplished through knowledge or use of computer technology.

The software piracy, theft of hardware, theft of time and services, hacking and electronic trespassing and the spreading of computer viruses are the examples of computer crime.

TYPES OF COMPUTER CRIME:

Software Piracy:

It is illegal duplication of copyrighted software. Millions of computer users have made copies of programs they don‟t legally own. Unfortunately, many people are not aware that copying software is the violation of Pakistan‟s criminal laws which protects intellectual property.

THEFT OF HARDWARE:

Computer hardware, such as microcomputers and printers, have always been valuable items that individuals could steal and resell.

Professional criminals can steal a laptop or cellular phone from someone‟s car.

THEFT OF TIME & SERVICES:

The theft of computer time is more common than you might think. Probably the biggest use of it is people using their employer‟s computer time to play games. Some people also may run sideline businesses.

HACKING & ELECTRONIC TRESPASSING:

A hacker is a person who enjoyed learning the details of computer systems and writing clever programs referred to as hacks. Hackers were, for the most part, curious, enthusiastic, intelligent, idealistic, eccentric and harmless.

Now a days they enter corporate and government computers using stolen passwords and security loopholes and steal information, transfer money to their accounts, and do a lot of other criminal activities. Many hackers cover tracks and leave without a trace.

COMPUTER VIRUSES:

A computer is a program designed to alter or destroy the data stored on a computer system. Computer viruses can be passed from one computer to another on floppy disks, over networks, and over remote modem connections. Spreading a virus may begin as a joke but may cause considerable damage.

COMPUTER VIRUS:

Introduction:

The term was first used by Fred Cohen in 1984.

Definition:

A computer virus is a small program that attaches itself to another program and attacks other software by making copies of itself.

A virus executes when an infected program is executed. Therefore only executable files can be infected.

Computer Viruses are Small:

Virus programs, like the infections microorganisms that are their namesakes, are often small. Only a few lines of program code are required to write a simple virus. The implication is clear: viruses can be easily hidden in healthy software and therefore prove very difficult to find.

Destructive Non-Virus Programs:

Aside from viruses, there are other threats to user systems, including:

- ★ Worms
- ★ Trojan Horses
- ★ Logic Bombs

As well as being potentially destructive by themselves, each can also be used as a vehicle to propagate any virus.

Worms:

A worm is a program (usually stand-alone) that worms its way through either the computer‟s memory or a disk and alters data that it accesses. It is different from a computer virus since it does not require a host. For example, suppose a worm program instructs a bank‟s computer to transfer funds to an illicit account. The fund transfers may continue even after the worm is destroyed. However, once the worm invasion is discovered, recovery is much easier because there is only a single copy of the worm program to destroy since the replicating ability of the virus is absent. This capability may enable it to re0-infect a system several times.

Trojan Horse:

A Trojan Horse is a destructive program that has been disguised (or concealed in) an innocuous piece of software.

Worm and virus programs may be concealed within a Trojan Horse.

Trojan Horses are not viruses because they do not reproduce themselves and spread as viruses do.

Logic Bombs / Time Bomb:

A program that is activated or triggered after or during a certain event. This may be several executions or on a certain day like Friday the 13th.

Writing a logic bomb program is similar to creating a Trojan Horse. Both also have about the same ability to damage data, too. Logic bombs include coding similar to that used in logic bombs, but the bombs can be very destructive on their own, even if they lack the ability of the virus to reproduce. One logic bomb caused problems in the Los Angeles water department‟s system. (or download) the software and run it.

Rabbit:

Replicated itself without limit to exhaust a resource

Types of Viruses:

There are several different types of viruses that can infect PC systems including:

- ★ Boot sector viruses
- ★ File infecting viruses
- ★ Polymorphic viruses
- ★ Stealth viruses
- ★ Multi-Partite viruses
- ★ Macro Viruses

Boot Sector Infector:

Hides in the boot sector of a disk or the partition table of a hard disk and takes over control of the computer system when it is booted. It then copies itself into the computer‟s memory. When other disks

are used, the virus transfer to their boot sectors. The most common boot sector viruses are the Pakistani Brain virus and the Stoned/Mariuana virus.

Application Program Infector:

The most infectious type of computer viruses is the application program infector or file virus. They may attach any executable file usually.COM and .EXE files. An application program infector takes control after the initial use of the infected program. Once the virus is in place in the RAM of the computer is shut off. The most widespread virus today is the Jerusalem virus.

Stealth Viruses:

Viruses which attempt to hide their presence. Some of the simple technique include hiding the change in date and time and hiding the increase in file size. Some even prevent anti-virus software from reading the part of the file where the virus is located. Some also encrypt the virus code using variable encryption techniques.

Polymorphic Viruses:

Change their appearance with each infection. Such encrypted viruses are usually difficult to detect because they are better at hiding themselves from anti-virus software. That is the purpose of the encryption.

Dark Avenger Mutation Engine:

Polymorphic encryption program used by virus developers to encrypt the virus in order to avoid detection. The engine use a special algorithm to generate a completely variable decryption routine each time. No three bytes remain constant from one sample to the next.

Multiparite Virus:

Virus which infects both the boot sector of a disk as well as application programs. Multi-particle viruses are the worst viruses of all because they can combine some or all of the stealth techniques, along with polymorphism to prevent detection.

Macro Viruses:

Virus which attaches to a word processing or spreadsheet file (typically a MS word or Excel file) as a macro. Once the file is accessed, it replaces one of the word or Excel standard macros with an infected version which can than infect all subsequent documents.

Preventing Infection:

Viruses pose a serious threat to computer systems. Thousands of viruses are in existence and more are being written each day and also some of them are self-
modifying and these all viruses making difficulty to protect the computer.

Many good antivirus programs, often called vaccines are available at minimal cost. Also some new microcomputers include built-in virus protection capabilities. Some virus programs can continually monitor the computer system and provide an alert or even lock the system when any unusual activity occurs. Some popular antivirus programs include the following:

- ★ McAfee Virus Scan
- ★ Norton Antivirus
- ★ NOD 32 Antivirus
- ★ Avast Antivirus
- ★ Avira Antivirus
- ★ Symantec Antivirus

New viruses are appearing all of the time so no program can offer absolute protection against them and virus utilities are constantly updated. But with the help of antivirus programs we can secure the computer systems very much.

COMPUTER SECURITY:

Computer security refers to protecting computer systems and the information they contain against unwanted access, damage, modification or destruction.

NINE RULES FOR DATA SECURITY:

1. Establish data security policies.
2. Establish password management procedures.
3. Control uploading of programs.
4. Test new or upgraded software in an isolated computing environment.
5. Purchase software from reputable sources.
6. Never leave a network workstation unattended.
7. Back up data and programs on a regular basis and store them off site.
8. Establish an effective disaster recovery plan.
9. Practice "Safe Computing".

Computer owners and administrators use a variety of security technique to protect their systems.

PHYSICAL ACCESS RESTRICTIONS:

One way to reduce the risk of insecurity is to make sure that only authorized personal have access to computer equipment. Organizations use a number of tools and techniques to identify authorized personnel.

★ PASSWORDS:

A password is a special word, code or symbol that is required to access to computer system. Passwords are the most common tool for restricting access to computer systems. Passwords are Many systems use passwords to restrict users so they can open only files related to their work. Many companies use call back systems, when a user logs in and type a wrong passwords, the system hangs up.

★ DIGITAL SIGNATURES:

A digital signature is a string of characters and numbers that a user signs an electronic document being sent by his or her computer.

The receiving computer performs mathematical operations on the alphanumeric string to verify its validity. One person creates the signature with a secret private key, and the recipient reads it with a second, public key.

★ FIREWALLS:

A firewall is a gateway with a lock; the locked gate is opened only for information packets that pass one or more security inspections.

★ ENCRYPTION:

Encryption is the encoding of data by converting the standard computer code into a secret code for transmission. After transmission, the data is converted back into standard computer code.

★ AUDITS:

Audit-control software is used to monitor and record computer transactions as they happen so auditors can trace and identify any suspicious computer activity.

★ MAKING BACKUPS:

Making the another copy is called backup.

PRIVACY:

Privacy refers to the right to keep personal information from being used for purposes for which it was not intended.

SOFTWARE PIRACY & LAW:

Law:

Laws are formal of conduct that a sovereign authority, such as a government, imposes on its subjects or citizens.

Copyright:

Pakistan‟s Copyright Law prohibits reproduction of software (Amendment) Act of Pakistan, 1992 (The Amendment Act) is now extended to cover computer software. It is illegal to make or distribute copies of computer without authorization. No other copies may be made without specific authorization from the copyright owner.

Penalty:

Pakistan‟s Copyright Law prohibits reproduction of software without permission from the owner of the copyrighted computer program. If caught with pirated software, you or your company may be prosecuted under the provision of the Copyright Laws. The penalties under the law include a fine of up to Rs.200,000 seizure of products used for illegal copying and a prison sentence of up of three years.