

# Chapter Eleven

## The Risks of Computing

## **11-1 Protecting Your Data or computer**

Because lives have become so dependent on computing, users are vulnerable to computers or specific data on the computer, being stolen or damaged. The cost of repairing or replacing computer equipment is a concern. The interruption of services and the replacing of lost information often cost a lot more than the equipment. Having your data stolen is a big concern for users on the Internet, regardless of whether it is through someone “hacking” into a computer or a matter of copyright infringement.

**Theft** There are many steps one can take to protect computer equipment against theft. There are systems where by you can lock computers in special cabinets or, by using durable cables, tie them to the desk. Video camera surveillance is very effective for areas with a large number of computers like central offices and network rooms.

**Damage** The same common sense rules apply as for any other equipment regarding physical damage.

**Data Loss** Losing your data can occur through hackers, hardware failure, power spikes, accidental deletions, or disgruntled employees. If you provide a critical service, you should have an emergency plan in place to cope with the loss of your system. This includes having backup copies of the data offsite, access restrictions for network users, and security measures to prevent unauthorized people from entering your computer or network.

**Backups** Your data should be backed up regularly and the backup copies stored in another location. Only the data needs to be backed up as the application programs can always be reinstalled from the original media. Also consider having backup copies of the application programs in case the original media is no longer available or works.

**Power** Computers are vulnerable to two kinds of power problems: outages and surges. If there is a sudden loss of power, the computer will shut down but you are likely to lose the information that you have been working on since you have last saved your work. In most cases this is mainly an inconvenience. Having an uninterruptible power supply (UPS) can provide some protection against total data loss. The more crucial your data, the more features should be available with the UPS and you should also have an emergency power generator. These are usually diesel driven. For example, most hospitals, traffic systems, and business organizations like stock exchanges or air traffic control systems would have emergency generators

## **11-2 Understanding Data Security**

In most cases, the data on computer systems is worth more than the computer equipment because it represents work that the organization has done. If a bank loses the data of its clients or an airline loses the data of its flight bookings, it would be catastrophic. Loss of data can have a long term effect on a company and the confidence of its clients. Data loss often has a ripple effect throughout other organizations that are related to, or do business with, your organization. A hacker is someone who gets unauthorized access to another computer, generally with the purpose of “looking around”, stealing, or corrupting data. Depending on who you speak to, this term was coined by the media to apply to anyone who created a program to break into a computer where they have no access rights. Some hackers refer to these people as “crackers” as they consider themselves to be very good with

programming languages or computer systems, and they are writing programs to test the security of another system. Regardless of the term, take precautions to prevent anyone from entering your system who hasn't been authorized, as a hacker could:

- steal information (like designs or project information) to sell
- destroy information in order to damage your company's ability to deliver products, services, or projects on time
- change information to cause embarrassment or to affect the company's reputation negatively
- Hackers could enter your premises and use one of the workstations, either physically or online. Physical security including access control, identification tags, and video surveillance are important tools to counter hacker attack. If your network is connected to the Internet or some other WAN, it represents another way a hacker can get access to your data. The first level of protection is to use firewall technology.
- An important technique to protect data is to use passwords. You can limit access to critical information by placing it in a folder on the server that requires a user ID and password to access. One should have a strategy to make it difficult for hackers to guess your password:

–Rather than use your nickname or your spouse's name, use logical but less obvious words,

e.g., your first name and the current month.

–Using a combination of letters and numbers is much harder to guess.

–Passwords should be changed regularly.

–If you're worried about remembering too many passwords, alternate between three and five

passwords, and be sure to keep them in a safe location.

–Try to use a different password for confidential files than the one you use for logging into the network or the Internet. This will ensure that the files remain protected, even if someone can guess your password to enter your system.

–Check with your network administrator or the ISP about casing on passwords. Sometimes these may be restricted to all lowercase, or it may not matter which casing you use. The importance of passwords should be impressed upon employees and that passwords should be used carefully. Although it is harder to remember, it may be a good strategy to use different passwords for different files, network access, and your Internet accounts.

The common image of a hacker is of a young individual, typing away frantically in a dark basement, etc. In reality, most hackers are very ordinary people. They normally gain access by getting the necessary user ID and password from an employee, friend, or disgruntled employee. Data security is a very specialized field. Most companies will use a security consultant to do a risk assessment and recommend an appropriate security plan for the company. The plan should also include training for the employees.

### **11-3 Establishing Safe Working Environment**

- Avoid temporary setups for the computer as they tend to last much longer than intended. A monitor placed on top of several telephone directories is not a safe location as the monitor can be knocked off its pedestal if someone bumps the desk. Place monitors on stable desks and position the wiring appropriately.

- Ensure your CPU is positioned somewhere where it is stable such as the floor or a very solid table, and that there is ample space behind the CPU for air circulation. Remember that the CPU has a fan that cools down the computer. On occasion you may also want to remove any dust buildup in the computer and the fan. Vacuums or air pressure tools designed for the computer can be purchased for these tasks.
- Consider using a power bar to connect your computer to the power outlet. A good power bar should also offer surge protection with it. Be careful about overloading the power bar as this may cause power fluctuations to the computer. For example, a laser printer should never be plugged into the same outlet as the computer as they will compete for power and the printer will usually win! In this scenario, consider plugging the computer into a power bar that then plugs into the wall outlet and plug the printer into a different wall outlet, either via another power bar or directly to that outlet.
- Protect yourself and others from accidentally tripping on any cables by using proper tools to keep them neat and out of the way. If you can, avoid having cables cross a walk-through area, but if necessary, ensure the cables are covered with an appropriate cover. Consider purchasing the appropriate ties to hold the cables together rather than using twist ties or elastics.

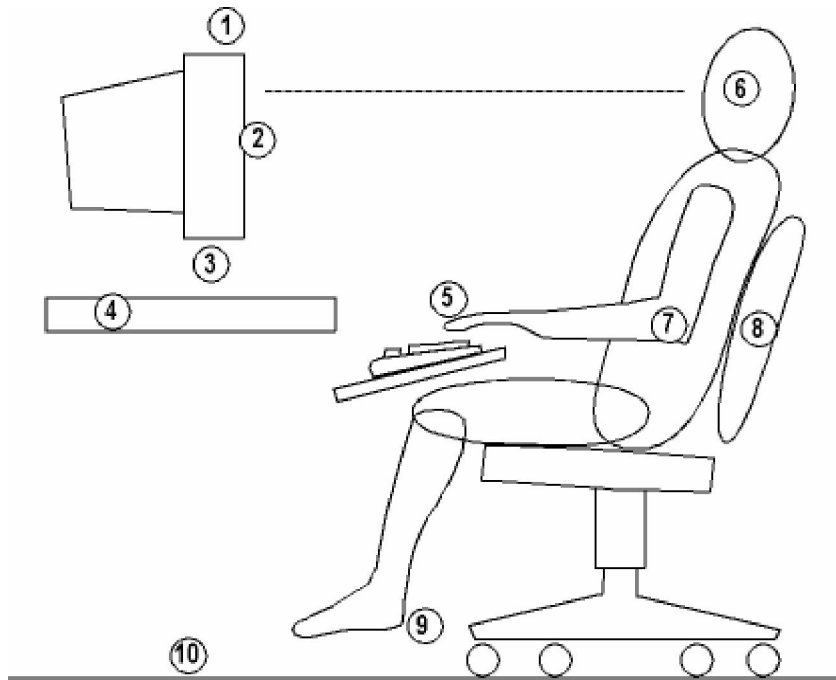
### **11-4 Using Ergonomics**

Ergonomics, or human factor engineering, is the study of the human in the workplace. Ergonomic studies have identified a number of potential problems relating to extended computer use. When working on a

computer, one tends to sit for long periods of time, looking at the computer screen, typing and using a mouse. We have probably all experienced back strain and eye strain while working with a computer. If you do this on an on-going basis, it could lead to a permanent disabling injury. By applying ergonomic principles and using proper equipment, the risk of injury can be greatly reduced. There are three particular areas of concern: the wrist and hand, elbow and legs.

- Frequent rapid motion, such as typing or using the mouse can cause repetitive motion injury (RMI).
- A similar situation can arise at the elbow joint.
- Sitting for extended periods on incorrect seating constricts the blood flow in the legs and applies pressure on the nerves. This can lead to swollen feet, painful nerve damage, blood clots and blood vessel blockages.

If you work at a computer for a few minutes a day, you need not really concern yourself too much with ergonomics other than your comfort. However, if you need to work for several hours per day, you need to keep ergonomics in mind. The first thing to do is never to work without taking regular breaks. Get up about once every hour, stretch and walk about to get the circulation going. The following will illustrate some of the main points to keep in mind when considering a computer workstation.



1 -The monitor and keyboard should be directly in front of you. You should not have to look or type at an angle.

2- There should be no glare or reflections on the screen.

3- Place any documents that you will be typing from in a document holder next to the monitor.

4- The work surface should be stable.

5- Once seated comfortably, your wrists should be straight and flat.

6- The top of the monitor should be about 2-3" above your eyes.

7- Your arms and elbows should be close to your body.

8- Use a good, adjustable ergonomic chair. Sit slightly back and not exactly upright. Sitting back in your chair in a reclined posture (with your back at around 110 degrees) is recommended for good lower back health.

9- Your feet should be flat on the floor when you are seated comfortably. Your upper legs should be more or less horizontal. If your feet cannot reach the floor then you need to use a foot rest.

10- Although not part of the workstation design, remember to take regular breaks – this will go a long way to avoiding injury!

### **Preventing Eye Strain**

Once you have a proper workstation layout, consider the following points to avoid eye strain:

#### **Viewing Distance**

The monitor should be at a comfortable horizontal distance for viewing, which usually is around an arms length (sit back in your chair, raise your arm and your fingers should touch

#### **Screen Quality**

A good quality monitor can go a long way to reduce eye strain, such as a monitor with high resolution so the characters will be sharp. There should be no visible flickering of the screen while you work.

#### **Bifocals and Progressive Lens**

You should be able to see the screen without tilting your head back or craning your neck forwards, even if you wear special lenses, provided you have followed the workstation guidelines.

#### **Proper Lighting**

Natural light is always better for clarity as well as general health. However, it may also cause glare on the screen if you have the monitor facing the window, and of course, when the daylight leaves, you will need another source of lighting. Where possible, the lighting should be above or behind you, facing onto the monitor. If you are using a desk lamp, never have the light source pointing toward your eyes; it should be aimed towards the monitor and the desk to provide light for the screen and any papers being reviewed.

## **Eye Checkup**

If you are experiencing eye strain, you should consult an eye professional.

## **Rest**

Again, remember that regular breaks go a long way to avoiding problems.

When you take a break, remember to look in the distance.

## **11-5 Viruses**

There is only one way that you can have a virus infect your computer — you let it in! The only way to know for sure whether a virus is a hoax is to check with your network administrator or a web site that lists different types of virus hoaxes before you send a warning message to anyone else. There are a number of sites that provide this information, including:

<http://securityresponse.symantec.com/avcenter/hoax.html>

[www.trendmicro.com/vinfo/hoaxes/hoax.asp](http://www.trendmicro.com/vinfo/hoaxes/hoax.asp)

<http://us.mcafee.com/virusInfo/default.asp>

[www.truthorfiction.com](http://www.truthorfiction.com) (this site also contains information about scam programs)

Looking at the Types of Viruses , Essentially there are four basic types of viruses that could attack your system:

### **1- Boot Sector**

As the name implies, this type of virus will infect your system when it is read from an infected floppy disk that has been set up as a boot disk.

### **2- Program or File**

In this case, the virus is part of a file that can be used to start a program or action (e.g., batch file).

### **3- Macro**

This type of virus looks like a macro file that will run in a specific program that uses macro languages (i.e., Microsoft Word or Excel).

#### 4- Multipartite

These viruses work similar to a boot or program virus except that these generally will infect both areas.

There are some other malicious viruses that exist, although they are not actually a virus (i.e., they do not actually fit into one of the previously mentioned types). Many of these can cause as much or more damage to a computer. The two most common types here are worms and Trojan horses.

#### **Worms**

These are virus programs that duplicate or replicate themselves through some means. Depending on the virus, it may be through infection of a program file, or as has been the case in recent years, through e-mail wherein they will re-send themselves to people in the recipient's contact or address list in their e-mail program.

#### **Trojan Horses**

These types of viruses are written to be “hidden” and appear harmless. However, they usually will activate when some action happens, e.g., on Friday the 13th when the program may blank the screen and move all the files to a hidden area of the computer.

### **11-6 Performing a Data Backup**

A backup is when you save your data elsewhere as well as the regular folder or hard drive. Then you can recover the data even if your computer was stolen, data corrupted or deleted, or if your computer is damaged by other means. The first strategy is to save regularly while you are working. Learn the habit! Many software programs can be set to do an automatic save at regular intervals — make use of that feature. Alternatively, you may have saved the file previously and all your data was backed up to a

CD. You no longer need the file and delete it from your hard drive. A few months later, you realize you want that file but it no longer exists on your computer. Having that backup copy on CD allows you to restore or copy it back onto your system from the backup copy. To protect the data, all users regardless of whether you are connected to a network or not, should be required to log into the computer using a valid id and password. This will help to reduce any damage that could occur if someone is able to enter the computer or network without proper authorization. Network administrators will also tend to force the users to change their password on a frequent basis in order to prevent others from being able to use your password with your login id. If the computer is stolen, then the data is lost whether you saved regularly or not. That is where backup procedures can come in handy. Every organization has a backup strategy.