UNIT 8 INFORMATION SYSTEM SECURITY

Structure

8.1 INTRODUCTION: ETHICS IN INFORMATION SOCIETY

Ethics determine generally accepted and encouraging activities within a company and the larger society. Ethical computer users define acceptable practices more strictly than just reframing from committing crimes. They consider the effects of their activities including Internet usage, on other people and organizations. There are many associations who have developed a code of ethics that provide useful guidance. The association for computing Machinery (ACM) has developed a number of specific professional responsibilities. These responsibilities include the following:

a) Access computing and communication resources only when authorized to do so.

b) Honor contracts, agreements and assigned responsibilities.

c) Give comprehensive and through evaluations of computer systems and their impacts, including analysis of possible risks.

d) Accept and provide appropriate professional review.

e) Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

The above code of conduct for his deeds if a person accesses some data without proper authorization, he held responsible. The person cannot say that data should have been protected and get away with it. The information system and their impact must be audited like other systems. Information system is like any other product and the users must be aware of the risks involved. The unethical use of information system can devastate an organization.

8.2 OBJECTIVES

After reading this unit, you should be able to:

- Describe ethical issues involved in information society;
- Discuss the right to privacy and freedom of information in society;
- Explain the need and mechanism to protect hardware and software from unauthorized access;
- Recognize the importance of having a disaster recovery plan; and
- Measure the threat of virus and identify ways of preventing them

8.3 INFORMATION RIGHTS, PRIVACY AND FREEDOM IN AN INFORMATION SOCIETY

Privacy is an important social issue involved in information society. Privacy deals with the collection and use or misuse of data. Data is constantly being collected and stored on each of us. This data is often distributed, sold or used without our knowledge. The health care provider and retail shops have, for instance, forms of data on its clients and customers. The fundamental question is "who owns this data and information?" We know for sure that we would not like to share our medical records with others, definitely not with insurance company or our employers.

The employer can use information technology to monitor the employees. The time spent by an employee on computer can be recorded along with his activities. The employer can use this data to estimate the number of breaks an employee takes. The employer can easily monitor electronic communication in the form email. At the same time, an employee can reveal company data to monitor employee's emails. The deleted emails can be retrieved and used as evidence if required.

Privacy of hardware and software consumers is another important issue. If hardware companies give a unique identification to each major component, the software company can use this number to uniquely identify each electronic documents created. This could be useful in checking the piracy of users is compromised. Ethernet card is the only hardware component that has unique identification, which is used in communication. The Indian Constitution of 1950 doesn't expressly recognize the right to privacy. However, the Supreme Court first recognized in 1964 that there is a right of privacy implicit in the constitution under Article 21, which states, "No person shall be deprived established by law".

8.4 PROTECTING COMPUTER EQUIPMENT AND FILES

Crimes involving illegal system access and use of computer services are also a concern. The systems left unattended over weekends without proper security have been used for commercial use. Computer magazines regularly report cases where employees have used the facilities for their personal benefit sometimes at the cost of their employers.

Hackers make use of their computer knowledge to gain access to others computers. Sometimes, files, passwords, programs, or processing power are stolen. An intruder may alter the data or destroy the data making it unusable and useless. A hacker writes a small password snifter that is hidden from the computer owner. A password snifter can steal passwords and gain access to data and files. There are Antisniff Programs that can detect and block a password snifter.

All types of computer systems and equipments have also been stolen from offices. In one recent incident, all hardware components from the computer age were removed and carried away, leaving the cage behind.

8.5 LIMITING LOGICAL ACCESS TO COMPUTER SYSTEMS

Personal efforts can reduce the risk of unauthorized access. You must protect your computing facility in the same manner in which you protect valuables. You must follow safety and security policies of your organization. For instances, you may be advised to change your password frequently and choose password carefully. In case your organization does not have a written policy, it is time to create written computer security policy. In case, an incidence takes place, treat it the way you would treat any other theft. Inform the authorities, document the incidence as accurately as you can, back up all you files and data immediately and keep them offline. You must secure any evidence.

At corporate level, efforts to safeguard data and files include installation of specialized hardware and software. For instance, data and information are encrypted to prevent unauthorized use. Use of biometric is also becoming popular to authorize employees. There was one time when criminals were identified using fingerprints. The fingerprint identification has been extended to identify authorized users. Iris and retina scans which use to be part of science fiction movies has now become part of sophisticated identification methods. The latest is use of magnetic card that is checked by a magnetic card reader to allow entry.

Depending on the nature of the computer crime that an organization anticipates, it may adopt controls. The controls are expensive to implement and the organization must evaluate the cost against the benefit. To summarize, here is a list of control guidelines:

a) Install strong user authentication and encryption capabilities on your firewall.

b) Upgrade your software with the help of patches, which are developed by vendors whenever a security gap is found in the software.

c) Guest logins are always misused. Any book on Microsoft products advises against creating a guest login. Group accounts such as head-sales should also be avoided. Such accounts become public very quickly and no body can be held responsible. In one of the academic institute of India, head-department account was lying dormant for some time. A hacker noticed and started using it for surfing the net and providing access to others as well. He used 60 hours of download time per day for a month. At the end of the month, data is regularly checked when this got caught and the only solution was to de-activate the account.

d) Remote-logins also create serious threat to security. This fact is so well accepted that Linux does not permit super-user remote-login. There was a time when system accepted login and then prompted for password. While you typed password, a star will substitute each character. A person from a distance could easily learn the login and number of characters in the password. Systems have now changed and login-password is accepted together.

e) It is a good idea to have dedicated servers for applications that communicate with outside world. Encourage people to have separate passwords for Intranet and Internet if possible.

f) In certain cases, the law requires that audit trail must be on. A document once created cannot be changed without leaving an audit trail. Most of the ERP packages, for instance, leave audit trail. In case of a crime, the audit trail can be of immense hel.

8.6 DISASTER RECOVERY PLAN

An information system performs key functions for an organization. It for some reason, the system becomes non-functional for some time, the consequences may be unacceptable. Organizations usually have a set of emergency procedures for critical functions. In best scenario, the end user will not be able to discover the failure of regular system. Generally, the switching to alternate mechanism and procedures is not seamless and the switching causes certain level of inconvenience to the users. For instance, a library may issue books recording them manually if the information system becomes temporarily unavailable.

The main reasons for system failures include power failure, data corruption, disk failure, network failure etc. Nature also plays its role sometimes in the form of a fine, flood or earthquake. In addition, labour unrest or human errors may also render system unusable.

One of first stops of disaster planning is to identify threats. Not all the threats listed earlier will be a concern to an organization. After identifying the threats, appropriate disaster recovery plans should be implemented. We discuss disaster recovery plans next.

Hardware backup

In case of a natural disaster or due to technology failure, the hardware may become unusable. There are companies and firms that provide disaster recovery services. A company may provide a hot site that has an operational ready to use system. This is an expensive option, as the system is kept up to date, usually in different seismic zone. The next option is to maintain a cold site. A cold site provides the infrastructure but not the processing power and data. In case of a problem, the backup system is made operational.

Some companies provide data backup services. You can keep a copy of your data in electronic farm.

Software Backup

Software programs are precious assets of an organization that must be protected. A human error may delete a software package or a hardware failure may make it inaccessible. A simple strategy is to make copies of software and keep them safely. In addition, one may like to keep another copy of-site in a safe environment.

The least one should do is take regular backup. If the data is too large, incremental backups can be taken or selected data may be backed up at regular intervals.

The smart strategy is to be in pro-active mode rather than reactive mode. It may be less expensive to plan ahead to avoid possible down time than suffer losses.

8.7 COMPUTER VIRUS AND PREVENTION

A virus is a program that reproduces itself, usually without your permission or knowledge. In general terms, they have an infection phase where they reproduce widely and an attack phase where they do whatever damage they are programmed to do (if any). There are a large number of virus types. Another way of looking at viruses is to consider them to be programs written to create copies of them-selves. These programs attach these copies onto host programs (infecting these programs). When one of these hosts is executed, the virus code (which was attached to the host)

executes, and links copies of it-self to even more hosts. Many viruses do unpleasant things such as deleting files or changing random data on your disk, simulating typos or merely slowing your PC down; some viruses do less harmful things such as playing music or creating messages or animation on your screen. Such activities steal system resources.

Virus writers have to balance how and when their viruses infect against the possibility of being detected. Therefore, the spread of an infection may not be immediate. Some viruses infect other programs each time they are executed; other viruses infect only upon a certain trigger. This trigger could be anything; a day or time, an external event on your PC, a counter within the virus, etc. Virus writers want their programs to spread as far as possible before anyone notices them. In order to avoid detection, a virus will often take over system functions likely to spot it and use them to hide itself. Such viruses are known as Stealth viruses. A virus may or may not save the original of things it changes so using anti-virus software to handle viruses is always the safest option.

Polymorphic viruses change themselves with each infection. There are even virus-writing toolkits available to help make these viruses. These viruses are more difficult to detect by scanning because each copy of the virus looks different than the other copies.

Viruses often delay revealing their presence by launching their attack only after they have had ample opportunity to spread. This means the attack could be delayed for days, weeks, months, or even years after the initial infection.

The attack phase is optional; many viruses simply reproduce and have no trigger for an attack phase. However, these viruses write themselves to the disk without your permission to steal storage and CPU cycles. These viruses often damage the programs or disks they infect. This is not an intentional act of the virus, but simply a result of the fact that many viruses contain extremely poor quality code.

As an example, one of the most common past viruses “Stoned” is not intentionally harmful. Unfortunately, the author did not anticipate the use of anything other than 360K floppy disks. The original virus tried to hide its own code in an area of 1.2MB diskettes that resulted in corruption of the entire diskette. This bug was fixed in later versions of the virus.

There are currently over 50,000 computer viruses and that number is growing rapidly. Fortunately, only a small percentage of these are circulating widely. A virus’ name is generally assigned by the first researcher to encounter the beast. The problem is that multiple researchers may encounter a new virus in parallel, which often results in multiple names.

However, viruses are only one way your data can be damaged. You must be prepared for all threats; many of which are more likely to strike than viruses such as disk failure due to hardware problem. There are many other threats to your programs and data that are much more likely to harm you than viruses. A well-known anti-virus researcher once said that you have more to fear from a cup of coffee (which may spill) than from viruses. While the growth in number of viruses and introduction of the Microsoft Word® macro viruses and Visual Basic Script worms now puts this statement into question (even though you can avoid these by just not clicking on them to open them!), it is still clear that there are many dangerous occurrences of data corruption from causes other than from viruses.

So, does this mean that viruses are nothing to worry about? Emphatically, no! It just means that it’s foolish to spend much money and time on addressing the threat of viruses if you’ve done nothing about the other more likely threats to your files.

Because viruses and worms are deliberately written to invade and possibly damage your PC, they are the most difficult threat to guard against. It's pretty easy to understand the threat that disk failure represents and what to do about it (although surprisingly few people even address this threat). The threat of viruses is much more difficult to deal with. There are no "cures" for the virus problem. One just has to take protective steps with anti-virus software and use some common sense when dealing with unknown files.

Finding a virus on your system may not be easy; they often don't cooperate. Using anti-virus tools is important.

A virus may or may not present itself. Viruses attempt to spread before activating whatever malicious activity they may have been programmed to deliver. So, viruses will often try to hide themselves. Sometimes there are symptoms that can be observed by a trained casual observer who knows what to look for.

Virus authors often place a wide variety of indicators into their viruses (e.g., messages, music, graphics displays). With DOS systems, the unaccounted for reduction of the amount of RAM known of a computer is an important indicator of presence of a virus. But, under Windows, there is no clear indicator like that. The bottom line is that one must use anti-virus software to detect and fix most viruses.

Your main defense is to detect and identify specific virus attacks to your computer. There are three methods in general use. Each has pros and cons. Often, a given anti-virus software program will use some combination of the three techniques for maximum possibility of detection; namely Scanning, Integrity checking and Interception. We briefly look at scanning next.

Once a virus has been detected, it is possible to write scanning programs that look for signature string, which is a characteristic of the virus. The writers of the scanner extract identifying strings from the virus. The scanner uses these signature strings to search memory, files, and system sectors. If the scanner finds a match, it announces that it has found a virus. This obviously detects only known, pre-existing, viruses. Many so-called "virus writers" create "new" viruses by modifying existing viruses. This takes only a few minutes but creates what appears to be a new virus. It happens all too often that these changes are simply to fool the scanners. Newer scanners often employ several detection techniques in addition to signature recognition. Among the most common of these is a form of code analysis. The scanner will actually examine the code at various locations in an executable file and look for code characteristic of a virus. A second possibility is that the scanner will set up a virtual computer in RAM and actually test programs by running them in this virtual space and observing what they do. These techniques are often lumped under the general name "heuristic" scanning. Such scanners may also key off of code fragments that appear similar to, but not exactly the same as, known viruses.

The major advantage of scanners is that they allow you to check programs before they are executed. Scanners provide the easiest way to check new software for known or suspected viruses. Since they have been aggressively marketed and since they provide what appears to be a simple painless solution to viruses, scanners are the most widely used anti-virus product.

If too many people depend solely upon scanners, newly created viruses will spread totally unhindered causing considerable damage before the scanners catch up with the viruses. An example of this was the attack by the Maltese Amoeba (Irish) virus in the UK. This virus was not detected prior to its destructive activation on November 1, 1991. Prior to its attack, it had managed to spread quite widely and none of the existing (mostly scanner-based) products detected this virus.

Another major drawback to scanners is that it's dangerous to depend upon an old scanner. With the dramatic increase in the number of viruses appearing, it's risky to depend upon anything other than the most current scanner. Even that scanner is necessarily a step behind the latest crop of viruses since there's a lot that has to happen before the scanner is ready. The virus has to be detected somehow to begin with. Since the existing scanners won't detect the new virus, it will have some time to spread before someone detects it by other means. The newly discovered virus must be sent to programmers to analyze and extract a suitable signature string or detection algorithm. This must then be tested for false positives on legitimate programs. The "string" must then be incorporated into the next release of the virus scanner. The virus scanner or detection database must be distributed to the customer. If you depend upon a scanner, be sure to get the latest version directly from the maker. Despite the most extensive testing it is possible that a scanner will present false alarms (i.e., indicate a file as infected when it really is not).
Another line of defense is continuing education.

8.8 SUMMARY

In this unit, we have learnt about ethical issues involved in information society. We also discussed the right to privacy and freedom in information society. There is a need and mechanism to protect hardware and software from unauthorized access. You must understand the importance of having a disaster recovery plan and every organization should plan against a possible disaster. We also discussed the threat of virus and ways of preventing them.

8.9 UNIT END EXERCISES

1) Does an organization have a right to collect and share information without the permission of person concerned? What are the ethical issues involved in information society.
2) "Every component of a computer such as software, hardware and network should be protected". Justify!
3) Why should every organization have a disaster recovery plan to protect itself? What are the main components of a disaster recovery plan?
4) Write a brief note on virus threat and a protection strategy.

8.10 REFERENCES AND SUGGESTED FURTHER READINGS

Bishop Matt(2002), *Computer Security: Art and Science,* Addison-Wesley Pub Co; 1st edition.

Pfleeger Charles P & Pfleeger Shari L., (2002), *Security in Computing, third edition,* Prentice Hall PTR.

http://www.cknow.com/vtutor/vtintro.htm