Computers & Security, 16 (1997) 439-449

Procedures To Reduce The Computer Virus Threat

Harold Joseph Highland, FICS, FACM

Editor-in-Chief Emeritus

The computer virus threat early in 1988 resulted in a spate of recommendations of ways to reduce the danger of infection. Much of what was then written was based more on an emotional response than a rational understanding of the problem. Although laudable, many recommendations were platitudes and offered little assurance that a virus attack will be thwarted. Many recommendations were made without considering user reaction and/or work throughput.

First let us examine some of the *sensible rules* more carefully now that we have a better understanding of what was happening.

Rule #1: "Only use programs obtained from reputable producers."

Sounds great! But how about purchasing Freehand from Aldus and finding a virus inside the sealed plastic package? Or consider the users in the UK and Australia who received updates of their operating system from the friendly Amiga dealers only to find that the disks infected their systems. Then there was the reported incident in the Federal Republic of Germany. Dealers received a demonstration version of Apple's Multifinder to duplicate and give copies to their customers. The disk, unfortunately, contained a virus.

Rule #2: "Never use programs downloaded from a bulletin board."

True that this will reduce the possibility of a virus infection but not all boards are in the same class. Asking many users to give up these programs is asking them to spend needless money or do without some excellent utilities that they could not obtain from any other source.

Alert and reliable bulletin board operators could provide users with a checksum program. They can offer source code or send users a 'catalogue' of checksums for the programs they have on their system. A user can use a stand-alone special microcomputer solely for downloading such programs. It is possible to run a checksum on the copy received. If that checksum is incorrect, the user would immediately power down his/her system. The system should not be restarted for several minutes and the disk used in that case can be discarded or degaussed with a unit similar to those used with mainframe tape reels, to cleanse the possibly infected disk. In

0167-4048/97$17.00 © 1997 Elsevier Science Ltd

the States we have purchased standard floppy disks in bulk for about 25 cents each and would rather throw out a suspect disk. On the other hand, even though we pay only about 75 cents for high density floppies, we use a degausser.

Rule #3: "Implement procedures that prohibit employees from bringing programs from home into the office."

This should have been implemented months, even years ago. However, has anyone heard of a firm that fired an employee for doing so? Unless the rule is uniformly enforced against all employees no matter what position they hold, it is of little value.

Even though some firms strongly discourage employees from bringing their own programs into the office, many do not object to their employees taking work home. How secure is the firm's disk in the employee's microcomputer that may be infected? Will the disk, when returned to the office, be examined to make certain that it contains no virus?

Also in the States we have employees who attend colleges and universities after work, a program supported by many organizations. These employees often use the school's microcomputers, a strong source of virus infection. These same employees bring their 'school' disks into the office to do their homework during spare time.

Rule #4: "Use removable hard disks to reduce infection."

This technique does protect files on a disk from being accessed by others. It can be used in an environment in which highly sensitive data is isolated. However, this really offers no additional protection against a computer virus because it is as easy to infect a removable hard disk when it is being used as it is a fixed one?

Rule #5: "Use diskless workstations in a local area network."

From a top management viewpoint, one could ask if you do not want the user to have his/her own floppy disks, then why were microcomputers purchased in the first place? It would have been cheaper to have purchased a minicomputer with workstations in the beginning. Furthermore, there is an employee retraining problem. The suggestion to use diskless workstations has merit only in an operating environment in which there is no control over employee actions.

How To Reduce The Computer Virus Threat

The development of a program to reduce the risk of damage from computer viruses requires that such a program is:

[a] supported by administrative management,

[b] be part of the total computer security programme, and

[c] supplemented by a user awareness programme.

It is essential that company policies dealing with microcomputer security should be clearly stated in a printed manual distributed to all employees. These policies should be enforced uniformly and not have one set of rules for management and another for secretaries, data entry clerks, etc.

Also, combatting the computer virus threat will require a change in user work habits. Unless management is willing to accept some decrease in employee output, at least for the near term, there is no assurance that any formulated programme will succeed.

Likewise employees must accept the work procedure changes for the programme to succeed. An employee education programme is a critical element. We do not propose turning users into technical specialists but we do propose that certain everyday routines be modified and followed.

Is There a Virus in Your System?

How do you know when there is a computer virus in your system? Although many of the anti-virus products will undoubtedly warn you about an illegal operation, a tell-tale sign of a computer virus, not all warnings are really computer virus attacks. During 1988 and 1989 we have had numerous telephone calls from individuals who were sure their systems had been attacked. Many of these attacks turned out to be false alarms. In most cases the attacks were caused by human oversight or carelessness.

There are however several indicators that you might watch. Some are warnings of incompatibility of programs, others are operator errors, still others are signs of equipment malfunction, but some may be warnings about a computer virus attack.The following are some of these indicators.

- **The number of files on the disk has increased**

Every time you add a program or directory on your hard disk make a printout of the disk's directory and keep it handy. If you obtain a directory of the disk at some stage during operation and find that the number of files has increased, stop! Did you create a new file or files during the execution of some program? Did you forget to update your master list recently?

If you are certain that you have not modified the amount of disk space used by adding new files, compare the two directories. Search for new file names. Are they familiar? Examine the contents of the suspect files using the Norton Utilities or PC Tools if you have sufficient knowledge. Otherwise, call for help.

- **The message "1 File(s) copied" appears even though no COPY command was invoked**

Stop! Have you used a .BAT file which invokes the COPY command as part of its procedure'? If not there is a good chance that a virus is in the system.

- **The amount of RAM space in the system becomes smaller**

At boot time run CHKDSK or any other utility to determine the system's RAM size. If later you rerun CHKDSK or the utility and find the number of bytes available in RAM has decreased, stop! Unless you have added a TSR during operations, chances are that a decrease in available RAM space spells trouble.

[Refer to actions suggested in the next two indicators.]

- **A file's date/time stamp has been changed**

No one is able to remember the date and time of each executable program and file on a disk, particularly a hard disk. However, if you find a recent date for any file, stop.

Recall if you recently created a new file or installed a new program. A few months ago we added a new program on the hard disk. During its automatic install program it creates four temporary files. Because the installation was aborted the program was unable to remove the temporary files. Even during normal installation that program would add its own .CNF [configuration] file with the installation date and a device driver

Compare that date with a listing you made earlier. Unless you or a new program has created recently-dated files, chances are there is a computer virus in the system.

- **The size of an executable program has increased**

Again it is necessary to refer to the directory listing of the clean system that you took earlier. Any change in program size should be suspect. Executable programs do not change in size unless they have become infected or otherwise corrupted.

- **Bad clusters appear on a disk**

Normally almost all hard disks come from the producer to the user with some bad clusters. Unless you know which ones are there originally, you will not be able to identify the new one or new ones. A formatted floppy disk should have no bad clusters. If there are any bad clusters on a floppy disk, it is usually an indication of a poor quality floppy disk or a possible malfunction of the disk drive.

Produce a printout of a map of your hard disk using the Norton Utilities or PC Tools and keep it handy. Also keep a list of the location of the bad clusters using a program such as BADSECT. Periodically obtain a map on the monitor screen and compare it with the original. Any change should be suspect.

When you format a floppy disk use CHKDSK to determine if there are any bad sectors. If there are, reformat the disk and check again. Also when you purchase a program that is on a floppy disk, obtain a map to determine if there are any bad clusters.

- **A program normally run will not load because of insufficient space in RAM**

If you have not added a TSR other than those usually used on the system, stop! Use CHKDSK or a RAM-size utility to determine amount of RAM available. Also use a directory listing to check the guilty program's size and date/time stamps and compare them with the original.

- **Programs take longer to load**

Few of us can be aware of minor time changes. However, if you feel that loading time is longer, stop! Terminate program execution and take a directory listing of the disk and compare the program's size in bytes and its date and time stamp with the original listing. Then power down and restart system with care, maybe you are impatient.

- **Execution time of a program takes longer than usual**

Sure you are not impatient? If not, follow the steps taken for longer program loading in the indicator above.

- **A disk drive light goes on when that disk is not being accessed for read or write during the current operation?**

This often means danger. Yet if you are in drive B and take a directory of a disk in drive A, the light on drive B will go on after the directory appears on the screen. Drive B is the default drive. This may also occur if the default drive is the hard disk C but chances are there may be no light visible on the C drive.

- **A TSR program fails to operate properly**

Did it work properly under the same conditions before? We have some TSR programs that cannot be called by hotkeys when other TSR programs are active. Known your system before you call for help.

- **Hard disk access time has increased appreciably**

Again this might be a case of time perception. Although something might be physically wrong with the drive you might possibly have a virus in the system. Power down and restart with a write-protected DOS disk in drive A. Run the hard disk diagnostic tests before you even attempt to look for a virus.

- **Program stops in the middle of execution and no disk lights are on, or the disk light remains on while the disk continues to spin on and on**

The system has apparently crashed; it can be caused by many things. After you have safely rebooted the system, examine the suspect program. Also run diagnostics on the disk drives. If nothing is found it could have been an equipment malfunction. Try to execute the program again. If it works, you are probably safe. Otherwise get special help.

- **Hard disk drive fails to boot**

Try booting the system from a write-protected floppy disk in drive A and obtain a directory of drive C. If no directory listing is possible, there is trouble. Otherwise, change the default drive to C and attempt to copy a text file from the hard disk to a clean formatted floppy disk. If it is not possible to copy the file, the hard disk is in trouble. Possibly the master boot record, partition table or file allocation table have been altered. Or possibly there is something physically wrong, such as the hard disk's heads. There is no question that you need technical help.

Guidelines To Reduce Risk Of Infection

1. **Check all NEW software**: All new software should be thoroughly checked for possible infection before it is installed on a hard disk or used with any programs and/or data on a floppy disk. Rules to examine software are noted in this section.

2. **Make backups on a regular basis**: This involves not only having a corporate policy concerning backups of programs and/or data files but also educating the users about viruses and computer security. Although a uniform corporate backup policy is essential, some data should be backed up more frequently than others.

3. **Keep master disks secure**:When adding a new software program to the system, make certain that the disk is write protected before inserting it into a floppy drive.This means covering the notch on the upper right side on a 5.25-inch floppy disk with a silver or black-on-silver coated write-protect tab. With a 3.5-inch disk, shift the plastic square in the upper right-hand corner so that you can look through the hole.

4. **Maintain regular checkups of the network**: The network administrator should carefully control all software programs put on the network. He/she should control the transfer of any executable program over the network. Because there is greater danger of the spread of a virus over the network, more frequent testing and precautions are essential.

5. **Do NOT permit users on a network to access outside bulletin boards**: No user should be able to download any material from an outside bulletin board or network. If such communication is essential for their job, no user should do so without special approval of the network administrator and only with appropriate safeguards.

6. **Reduce risks of infection by maintaining secure operating procedures and practices**: There is no 100 percent positive way to prevent an attack by a computer virus or Trojan Horse. Even with an anti-virus product there is always the risk of a computer virus being programmed to get around the protection device. Constant vigilance is necessary.

7. **Isolate an infected system at once:** If a system becomes infected or is suspected of being infected, stop processing on the system and/or network. The user should not attempt to replace the infected program and proceed with work. Follow the special procedure to restore the system!

8. **Get expert assistance at once:** Because computer viruses can spread rapidly and the typical user is not certain how to save critical data on the system, call upon an expert. In a large company, there should be a qualified individual who will perform the necessary work properly and safely. If one is not available, secure outside help.

Personnel to Improve Microcomputer Security

An increased number of employees must be involved in the microcomputer security program if any anti-virus program is to succeed.

[1] If a microcomputer security director [MSD] does not already exist in the organization, one should be appointed. Depending upon the individual's technical knowledge, it might be necessary to create a team with different technical skills to support the director. Do not assume that all current computer security personnel have the background to do this job.

[2] Following standard management principles an individual should be assigned to act as the microcomputer security administrator [MSA] for a department or a group of small departments. For very large departments, it may be necessary to appoint several individuals but make certain that one is put in charge. Select individuals, where

possible, with technical knowledge of microcomputing and not by their job title. It may be necessary to establish a training program to provide these individuals with an understanding of microcomputer security and improve their knowledge of the technical tools available to detect and respond to a computer virus attack.

[3] Create a software quality assurance section [SQAS] to test all software that will be used on the systems [this will be covered more fully later in this section].

Techniques to Reduce the Virus Threat

Even if an organization uses an anti-virus product there are several basic rules that should be followed that will lessen the likelihood of a computer virus attack. Some of these include:

[1] Standardize and control microcomputer hardware and software installation. This makes it simpler to evaluate software obtained by the organization. It has been found that speciality add-on boards and even different make add-on memory boards result in somewhat different program interactions. The greater the number of different configurations within an organization, the more time is needed to evaluate software programs.

[2] If specialized software packages are purchased for a specific department and/or set of users, that software should first be tested by the Software Quality Assurance Section [SQAS]. It should be isolated for specific users and not transferred to any other departments and/or microcomputers within the company. [Some testing techniques are contained later in this paper.]

[3] Strictly control access to microcomputers and control the programs that may be loaded and executed by specific users. This is part of normal computer security procedures. Consider the use of passwords or possibly tokens to access the machines and even the programs. If passwords are used, make certain that they are really changed frequently; follow standard password procedures when an employee is transferred out of a department or leaves the company.

[4] Keep executable programs on a disk without the related data; be certain to write-protect all floppy disks with programs.

[5] Do not permit individual employees to download programs from a bulletin board or bring their own software in from home. If they wish to download a program from a bulletin board, the request should be made to SQAS which should do so under established safety rules. Similarly, if an employee wishes to bring a utility from home, that utility should first be evaluated by SQAS before it can be used by the employee or anyone else in the company.

[6] Establish a backup policy that is based on the critical nature of the data kept within a department and/or by an individual and not necessarily on an overall, uniform time-dependent schedule.

[7] Even after SQAS approval, do not place downloaded or shareware programs in the root directory of a hard disk or on the file server of a LAN. [Most known computer viruses do not spread outside of the directory in which they exist.]

[8] When booting a floppy-disk system, always use a write-protected floppy disk. Prohibit the use of a floppy disk to boot a hard disk system except by security personnel.

[9] Caution every user not to use any programs received through the mails or from others, even those within the company, unless that program has been approved by the SQAS. This is particularly true for any package, even from a known producer, that has not been ordered by the user.

[10] Establish a policy covering the taking of any company disks home by an employee. Set up procedures to evaluate the disk when it is brought back to the office by the employee.

[11] Provide each employee with written recommendations to control the spread of computer viruses. Also give each employee information about how to spot a possible virus infection.

[12] Establish an ongoing user awareness programme under the supervision of the Microcomputer Security Director [MSD] in conjunction with the company's computer security director.

[13] If it is necessary to prepare data on one microcomputer that will be used on another system, copy the data on a non-bootable floppy disk. Do not copy any executable programs on the same disk.

[14] Supply each user with specific instructions about actions they must take if something unusual occurs and/or if they find a virus. Impress upon them that they should not continue using a microcomputer if the system has been attacked.

[15] Create a reaction/recovery manual or Red Book for each discrete system.

Acceptance of New Software

Even if a software package comes from a reliable vendor and is shrink-wrapped by the producer, the disks should be examined by the SQAS. This rule applies to every package whether it comes from IBM, Microsoft, Lotus or any other reputable producer. Until the Software Publishers Association develops a certification program that will assure the user that the purchased software is virus free, precaution is necessary.

In our organization, every software package received is analyzed on a protected microcomputer used for program testing and evaluation. There are eight steps in this procedure that we follow and strongly recommend for every organization.

[1] Obtain a map of each disk in the package to determine if the disk contains any bad clusters. If we find any bad clusters we notify both the producer and the vendor and return the entire package.

[2] If there are no bad clusters, examine each disk's boot sector to ascertain that it is a legal boot sector and does not contain a virus.

[3] Compare the list of programs printed in the documentation with those found on the disk. We use a special utility program to obtain that list rather than the DOS DIR command. If the list is not contained in the documentation, telephone the producer to obtain that list. If there are any unexpected programs on the disk, read them with a special utility and not under DOS. At this stage do not execute any program on the disk.

[4] Some producers are now including a special file that provides a checksum for each file on the disk and supply a program so that the user can generate checksums. Copy this program and all files from the purchased disk to a newly formatted floppy disk. With this floppy in the system and the hard disk write protected, execute the checksum program to obtain the checksum for individual files. Match the computed checksums with those provided by the producer.

[5] If there is a READ.ME file on a disk [such a file is often used by producers to provide up-to-date additions to the documentation], do not attempt to view it by using the DOS TYPE command. Instead read by using a special utility program.

[6] Similarly, read all .BAT files with the utility program before any attempt is made to execute the BAT files. If any of the statements in the file are not understandable communicate with the producer of the program to verify the contents.

[7] Use a utility program to examine the root directory on the disk. If there are any erased programs listed, verify with the producer that they are legally on the disk. Depending upon the technical proficiency of your staff, someone might restore the erased program or programs and examine them.

[8] Then and only then make backups of the disks. The original disks should be stored after an appropriate entry is made in a diskfile directory.

How to Handle Shareware and Freeware

Many shareware and freeware programs contain features not found in commercial packages and therefore provide useful utilities. However, their processing for quality assurance is more complex than commercial produced software. Often it is not possible to communicate with a producer and many of the safeguards found with commercial packages are missing. This therefore requires more exacting and time consuming examination and testing.

Some of the better bulletin board operators permit downloading of source code and provide a program checksum. If a program is downloaded, try to get the source code and compile it in house. If source code is not available, the executable program may have to be disassembled and analyzed.

Unlike commercially obtained software, these programs should be executed by the SQAS to determine interaction with other programs, especially TSRs generally used within the company. At no time should evaluations of this type of software be rushed. If the SQAS finds any unexplained actions during testing or the assembly code is questionable, the program should not be approved.

Finally, if the source of the software submitted by an employee is not known it is often safer to reject that program unless there is adequate time to do a complete analysis.

Operating Detection Techniques

Of course, steps must be taken to reduce the threat of a computer virus infection. Verifying the boot sector, the operating system, COMMAND.COM, CONFIG.SYS and the status of the interrupt vectors is a minimum. Checking floppy disks for date and size of COMMAND.COM and possible bad sectors is protection against the commonly known versions of the Lehigh and Brain viruses.

How about other steps? Using cryptographic checksums of executable programs and verifying them before and after the program is executed is another protective measure. Checking of the interrupt vectors and memory utilization before and after program execution is another useful technique.

Computer viruses have become far more sophisticated since the first days of the Brain and Lehigh viruses. Many of the anti-virus products have not been tested against several of the newer breed.

What to do if hit by a PC virus

If a PC system is actually infected by a virus, there are four areas in which actions are required:

[1] Minimizing the damage to the infected system.

[2] Minimizing the damage to other systems.

[3] Recovering the operation of the infected system.

[4] Assuring the infected system does not become reinfected.

The viruses with which the world at large is familiar, at least by name, the Pakistani/Brain, Lehigh and Israeli/PLO, are system or program infectors. With such viruses, data tends to be 'clean,' while various computer and/or disk areas are infected. It is these types of viruses that this writing considers. Although many of the recommendations, such as "stop using the microcomputer system immediately," would apply to any type of virus, other recommendations, such as "rebuild your system from original, shrink-wrapped diskettes and restore data from your most current backups" would not apply to virus-infected data or text files.

Things to Do:

- Immediately stop using your system! Forget about deadlines, the overlong time since your last backup and the like.
- If you are on a LAN, or are otherwise connected to other computers, immediately sever the con-

nection[s]. Do not worry about interrupted transmissions, open links, etc.

- Immediately notify every user, system and/or site with whom you have recently been in contact, either via disk transfer or telecommunications hookup, of your situation and symptoms. Do not do this over an infected system; use telephone, facsimile or possibly a virus-free network.

- Sound a general alert to every user companywide, or at least all users with even the most remote chance of contract with the infected system. Quarantine any and all systems with which the infected system came in contact until those systems are proven clean. Extend this to home computers if work goes off-site or users phone in.

- Do not use previously-used disks; they may be infected.

- Never save programs if a virus is present or suspected! Never execute a program on an infected hard disk! If you want to save certain data, shut down your system for several minutes, reboot from a write-protected system disk, and COPY files from the hard disk to floppies using the COPY command on the floppy disk. After this is done, clean and rebuild your system.

- If you want to be sure you are rid of a virus, clean your system. Cleaning involves wiping/overwriting your hard disks, doing a low level diagnostic format and restructuring your drive with FDISK. Next rebuild the system from write-protected original program disks, restoring data from your latest data backup. If you saved any data files from an infected disk write-protect these disks. Use a special text editor such as the Norton Utilities or PC Tools to examine each file carefully before copying any file[s] to the rebuilt system.

- Have every disk that may have come into contact with the infected system tested for viruses.

- Minimize contacts with other systems until you have tracked down the source of the virus or are secure in not being quickly reinfected.

- Maintain a dialogue with those you notified of your situation to determine their virus status.

- A major problem with a virus infection is the high probability of reinfection of the system. User logs of external contacts (network connections, diskettes in and out, others using the system) can go a long way toward minimizing the spread of the virus, and possibly even to tracking down the source. Such logs may be an automatic part of a general security product; certain anti-virus products offer them, too.

- Note: Several antivirus products claim to detect, and even remove, certain of the most frequently unspecified viruses. If you have access to such programs, you could try them at identifying your virus. I would not recommend the automatic removal by a commercial product at this time.

- Once you are back in operation, pay special attention to signs of virus activity.

The reinfection problem is probably the trickiest phase of the recovery procedure. Even if you accurately determine the type and source of a virus with which you have been hit, tracking down the other systems and floppy disks to which it may have spread [and which may, in turn, reinfect your system] is nearly impossible.

If you have access to a virus expert [and, if you have many PCS, or PCS are vital to your operations, you should make it your business to know of at least one such person on whom you can count]. He/she should immediately be called in. Such a person can be of immense help in identifying the type and source of the virus with which you have been infected, and can quite possibly devise automatic protection against the particular type and strain.

Jon David

Virus Disaster Red Book

Even if you use one of the anti-virus products to protect your system, you should be prepared to recover from an unexpected virus attack. Having had to reformat a 60-megabyte hard disk, create new partitions and set up the system's expanded and extended memory into RAM disks, we strongly urge anyone with a hard disk system, particularly those with complex configurations, to prepare a Virus Disaster Red Book now.

This manual should be created for each system and/or configuration (e.g. machines with different make on-add boards and/or hard disks from different manufacturers).

The following should be included in the Red Book:

[1] A complete listing of the sequential steps needed to install a new system. Next to each step is the number of the disk required, the program or programs to be executed and the keyboard input, if any, necessary to reply to the installation screens. Include in this listing a note to disconnect all communication lines, including those to shared printers, during the restoration procedure.

[2] A complete set of the required, write-protected disks to be used to boot the system from drive A; these should include the current operating system and all ancillary DOS programs. It should also include all disks needed to wipe the infected disk clean and those necessary to reformat the hard disk.

[3] A printout of a disk map of all the bad sectors that originally were present when the hard disk was purchased. If any sectors have gone bad since purchase, they too should be noted.

[4] A printout containing the sector/cluster location of all the bad sectors on the hard disk as noted in step 3 using BADSECT.COM or a similar utility;

[5] A printout of the partition table of the system's hard disk.

[6] A printout of the system's AUTOEXEC.BAT and CONFIG.SYS files.

[7] Copies of these files [5 and 6 above] on a floppy disk.

[8] Copies on a write-protected floppy disk of the system's drivers (e.g., SYS files, etc.);

[9] A printout of the root directory and all subdirectories, containing the following data:

[a] name of program,

[b] version number,

[c] name of source or supplier,

[d] length of file in kilobytes,

[e] date and time of the last update,

[f] checksum or CRC [cyclic redundancy check] of each program, and

[g] if source code is available, the number of lines of code in the program.

This list should be updated at least once a week, or in high activity operations, daily updating may be required.

[10] Copy of the backup program used to start the reloading of backup disks; both the backup program disk and the back-up disks should be write-protected during their use.

[11] A copy of a text editor, aside from DOS's EDLIN, if modifications to text is necessary during re-installation

[12] Copy of any communications program if used on the system.

[13] Copy of any access control software if the system is password protected.

[14] In special cases, a copy of the calendar, phone lists and memos if such is kept on the system; this should be updated daily.

[15] List of add-on boards and switch setting if present on the system.

[16] A disk that contains basic 'restoration' utilities including:

[a] the Norton WIPEDISK program used to write zeroes and ones over the entire hard disk before it is reformatted,

[b] the Norton NU program, and

[c] several Mace programs such as XFDISK, HFORMAT, HTEST, and RXBAK.

[17] If you use floppy disks to back up your system, use either The Norton Utilities or PC Tools deluxe to examine the map and boot sector of each backup floppy on another system prior to starting to backup the system being restored.

[18] Prepare a script for the recovery of data from an infected floppy disk.

[19] Maintain a list of user or staff suggestions to improve disk and/or program efficiency.

[20] Make a backup of all the material above and store that backup at a safe site.