TB40-0017
October 20, 1997

Computer Software Viruses

There has been much concern expressed recently by field personnel regarding software viruses. Computer viruses are the most insidious product of the computer industry and are a constant source of frustration for software developers. The Stratagy Voice Processing System is a personal computer-based voice mail system and as such, it is possible to infect the system with a virus. This bulletin outlines:

- what a virus is
- the steps Toshiba takes to protect its systems and software against viruses prior to shipping
- some steps that field personnel can take to ensure their systems do not get infected with a virus after they are installed

What is a computer software virus?

A virus is a piece of software specifically designed and written to adversely affect your computer by altering the way it works without your knowledge or permission. A computer virus is designed to replicate on its own. Computer viruses spread by attaching themselves to another program or to the boot sector of a disk. When an infected file is executed or the computer is started from an infected disk, the virus itself is executed.

One type of computer virus is a file infector. A file infector virus attaches itself to, or replaces, .COM and.EXE files; although in some cases, they can also infect files with other extensions. With these types of viruses, uninfected programs usually become infected when they are executed or when they are executed with the virus in memory. In some cases, the virus simply infects all of the files in the directory from which it was run.

Boot sector infectors are another type of computer virus. Every drive, both hard disk and floppy, contains a boot sector. This boot sector contains specific information relating to the formatting of the disk, the data stored on the disk and a small program called the boot program. The boot program is the program that gets infected by boot sector infecting viruses. Remember, because every disk has a boot sector, it is possible, and common, to infect a machine from a data disk.

Viruses can be attached to files that are accessed via the Internet or that are sent to electronic mail users. Literally, no one who uses computers is immune from computer viruses. Computer viruses don’t infect files on write-protected disks. They don’t infect compressed files either. However, applications within a compressed file could have been infected before they were compressed. Viruses don’t necessarily let you know that they are there, even after they do something destructive.

Computer Software Viruses

Toshiba Protection Standards

Toshiba takes extra steps to protect Stratagy systems and software from viruses.

Each master version of Toshiba software is examined for viruses using Norton Anti-Virus from Symantec™ and is then write protected. Even though write protecting the master version of software eliminates the possibility of it being infected with a virus, the masters are still periodically checked. Norton has several options that make it a valuable tool for virus detection. One of the most important options available to the Norton Anti-Virus software is the ability to update for the most current virus protection available over the Internet. Toshiba updates their files monthly.

Each set of software is scanned for viruses after it is produced. When the software is packaged, a sticker is placed on the anti-static bag stating the software is virus free. If you receive any software without this sticker, contact your Toshiba Dealer Sales Specialist.

Starting on September 15, 1997, Toshiba is shipping software on disks that do not have a tab in the write-protect window. This means Stratagy software disks can not be written to in the field, eliminating the chances of them being infected with a virus. Versions of software shipped prior to that date had the write-protect window closed. It is recommended you change the window to open so those software disks can not be written to. This will help protect the older versions of software.

What You Can Do

Toshiba strongly recommends:

- Copies of Stratagy software be made when the software is first received by the Dealer. Destination disks should be scanned first for viruses and the new disks write protected after the copies are made.
- Field personnel should have a virus checking software installed and running resident on their laptops. This means the software will automatically start when the laptop boots up and check the boot record for any known viruses. The software will also check the drives as new files are accessed. If the software finds any viruses, it should notify the user immediately and enable the user to fix the infected file. As new viruses are discovered at an alarming rate, the known virus files for the anti-virus software should be updated regularly.
- Any disks that are inserted in the A: drive of the Stratagy system should first be scanned for viruses. This will help reduce the likelihood of accidentally introducing a virus into the Stratagy that may have come from another PC. If the floppy disks are not being used to back up Stratagy files, the disks should be write protected.

There is no way to completely ensure that a PC does not get infected with a virus, as long as there are individuals who continue to write these destructive programs. By following these steps, the chances of your Stratagy systems being infected will be greatly reduced.