Virus prevention checklist

Recovering from a virus can be time-consuming and costly. To help you avoid such problems in the first place, use this checklist that includes options to consider when developing your virus prevention policies and plans. Of course, working environments differ, and it can be tricky to strike a balance between preventing viruses and hampering productivity. While a particular method may seem prudent to some people, others may view it as too cumbersome and restrictive. But the possibilities on this list should help you determine which strategies will be the most effective for you. These virus prevention methods are real-life examples of practices already in place.

Security settings

- ❑ Schedule regular backups of your data files.
- ❑ Protect your system(s) with antivirus software.
- ❑ Enable the virus-detection option in CMOS.
- ❑ If you have a firewall, make sure only necessary ports are open.
- ❑ Consider setting the attributes for critical system files (such as **SYS.INI**, **WIN.INI**, **AUTOEXEC.BAT**, and **CONFIG.SYS**) to read-only to prevent them from being written to.
- ❑ Windows NT administrators, set permissions to the registry and other system files to prevent unauthorized changes.
- ❑ Enable the virus expiration warnings to alert you when signatures are outdated.
- ❑ Set the server to scan both incoming and outgoing files.
- ❑ Include all file types when scanning, such as **EXE**, **DLL**, and **ZIP** files.
- ❑ Consider using a software package that allows files to be quarantined. This will prevent users from gaining access to the infected files and perpetuating the virus.
- ❑ If productivity will not be compromised, consider disabling the A drive of high-risk workstations from within a password-protected CMOS. If this is not feasible, disable the option of booting from the A drive.
- ❑ Set an audible alert when viruses are detected.
- ❑ Set user response options to the minimal acceptable level, such as “Cure” or “Quarantine.” Do not give the user the option to “Cancel” the repair.
- ❑ Enable all macro virus protection within software packages, such as Word and Excel.
- ❑ Edit the file-exclusion list so all **EXE** and **DLL** files are included during scanning. Some viruses target these files specifically.
- ❑ Create and maintain a write-protected emergency boot disk and know how to use it.

Signature updates

- ❑ Schedule regular updates of virus signature files. Most manufacturers offer updates on a regular basis—daily, weekly, biweekly, or monthly.
- ❑ Distribute the update to the workstations. If your NOS doesn't allow you to “push” updates to your users, consider sending it as an E-Mail attachment.
- ❑ Consider building the update into your users’ network login script.
- ❑ Consider purchasing Zenworks if you have no other mass-distribution options available. Zenworks will allow you to “push” these updates to your workstations.

- ❑ Make sure you update your write-protected emergency boot disk whenever new signature files are received.
- ❑ Consider setting up a dedicated server to retrieve your regular updates. Users can then connect to the internal server to update their workstations.

Diskette management

- ❑ Avoid using data and program disks received from unknown sources.
- ❑ Enact a policy that enforces the scanning of all diskettes before they are used in a workstation. You might want to set up a remote PC, perhaps an old 486, for this purpose.
- ❑ Consider providing a stockpile of virus-free diskettes for users to take home. Scan the disk upon re-entry to the workplace to ensure that the user's home PC is not infected.
- ❑ Write-protect all data and program diskettes.

Scanning

- ❑ Consider using a dedicated workstation that continually scans data directories on the network.
- ❑ Schedule full workstation scans on a regular basis with minimal intrusion to the user, such as during lunch or after hours.
- ❑ Perform scanning in "stealth mode" to achieve minimal intrusion to the user.
- ❑ Disable user intervention of scans.
- ❑ Enable background monitoring on the workstations.
- ❑ Determine if your browser offers a plug-in to scan files prior to downloading and use it if available. Netscape Navigator offers this in conjunction with Norton AntiVirus software.
- ❑ If a plug-in is not an option, make sure all downloaded files are scanned prior to installation.
- ❑ Smaller companies may want to document the date of the last "clean" scan of each workstation to alert the IT department at a glance.
- ❑ Scan new PCs received from vendors, as they have been known to contain viruses out of the box.

E-Mail policies

- ❑ Set E-Mail server filters to eliminate spam and unsolicited junk E-Mail that could contain a virus as well as malicious code.
- ❑ Set the server to immediately send a notification to the network administrator as well as the user. This will alert the user of the infected message before it is opened.
- ❑ Scan all incoming and outgoing E-Mail and attachments.
- ❑ Discourage non-work-related downloading of attachments.
- ❑ Do not allow users to forward jokes or chain letter E-Mail.
- ❑ Consider subscribing to a third party E-Mail scanning service. Infected E-Mail and attachments never enter your network.
- ❑ Call or E-Mail the individual who sent the infected E-Mail or document. They may not know they have a virus.

User policies

- ❑ Develop a system to educate all users about polices such as the "no download rule."
- ❑ Require that only the IT department perform all software installations.
- ❑ Do not allow your users to download or install shareware, such as games and screensavers.

❑ Create a rule that users should not bring diskettes from home, unless they are willing to allow the diskettes to be scanned by the IT department prior to being used.

❑ Consider limiting Internet access to approved sites. IE 5.0 allows an administrator to create a password-protected list of approved sites.

❑ Institute a set of applications that users have available to do their job. Do not allow any software to be installed beyond those provided with their system.

❑ Do not allow remote-access users to upload files to the network unless the IT department can verify the integrity of the PC being used for remote access.

Educate your users

❑ Publish links to reliable virus encyclopedias, such as Symantec's site at http://www.symantec.com/avcenter/ or Computer Associates' site at http://www.cai.com/virusinfo/encyclopedia/.

❑ Instruct your users to check these sites when they suspect they have a virus or when they want additional information. Users can also check for hoax virus information.

❑ Encourage users to install an antivirus software package on their home computers. Computer Associates (http://www.cai.com), one of the top antivirus software developers, offers their product, InoculateIT, free to home users (http://antivirus.cai.com).

❑ Encourage users to report when they find a virus on their system so you can track which viruses surfaced in your network.

❑ Consider developing an intranet site or Web site dedicated to virus information, with links to antivirus sites. If this is not an option, develop an E-Mmail newsletter that includes the same type of information.

❑ Inform your users of new virus threats. This will heighten their sense of awareness.

❑ Educate users on the proper use of macro virus protection. Instruct them to disable all macros when prompted unless the document has been given a clean bill of health and is known to be virus-free.

❑ Consider assigning offenders to an antivirus task force. Users found breaking policies or bringing a virus into the environment will be required to assist the IT Department in scanning workstations after hours.

Virus detection utilities

❑ Computer Associates—http://www.cai.com

Highlights:

- Monthly antivirus signature updates
- Hands-free downloads
- Antivirus E-News newsletter
- Free product updates
- Free personal antivirus protection with free signature updates
- Virus encyclopedia and hoaxes info—http://www.cai.com/virusinfo/encyclopedia/

❑ McAfee—http://www.mcafee.com

Highlights:

- Monthly antivirus signature updates
- Hands-free downloads
- Automatic updates and upgrades via subscription
- Free virus newsletter

- Virus encyclopedia—http://www.mcafee.com/viruses/virus_glossary.asp
- Virus hoaxes info—http://vil.mcafee.com/hoax.asp

❑ Symantec—http://www.symantec.com

Highlights:

- Weekly antivirus signature updates
- One year of free updates; $3.95/year thereafter
- Free product updates
- Virus encyclopedia and hoax info—http://www.symantec.com/avcenter/