Computer virus immunization

Simple steps to keep your company's risk of viruses at a minimum. **By Randy Wear**

Computer- and telephone-related technology needs to protect you, help you be more productive or increase your profits. It's that simple. Otherwise, don't spend money on it.

Computer viruses are rampant. Every day, talented and misguided people create viruses designed to steal resources from your computers, disrupt your operation, report on your computer use and confuse or damage your trading partners (since they often automatically replicate or spread to people you work with or e-mail to).

No one wants to spend money on the solutions, but the harsh reality is that there really is no choice. Dealing with the problems caused by getting a virus often costs clients thousands or tens of thousands of dollars, far more than preventing the virus from infecting them in the first place.

Even if you have no exposure to the Internet, your system can still get viruses. One large client received viruses on software media sent directly from the manufacturer.

Here are some steps you can take to mitigate your risk.

■ **Stop viruses before they get into your network.** Run antivirus software on your e-mail server, or to filter e-mail before it gets to your e-mail server. There is no sense clogging your network with viruses, so don't rely on PCs or Macs to detect e-mail viruses. Some ISPs that host e-mail offer anti-virus scanning of the e-mail.

But be aware — there is a difference between e-mail virus scanning and file/media virus scanning. You want both covered.

■ **Use a corporate or master edition of good antivirus software.** This will run on a server and push the antivirus software and updated libraries to all the other systems you want covered — and you should cover all your systems.

Symantec, Sophos, McAfee and a few others are the key, international software publishers to use. These corporate editions of the antivirus software automatically get updates and install them on each of the covered systems. This is very important. You can't rely on the users to get daily updates.

Clients who have tried having stand-alone, desktop antivirus solutions often find they have users who haven't gotten updates for a year. And they have viruses. The solution is to automatically install the updates.

■ **Set your antivirus servers to get updates at least daily, if not several times a day.** New viruses come out daily. You want to have the new libraries to get maximum protection.

■ **Be on the software publisher's maintenance plan.** You must be getting both software updates (to the core software) and the antivirus libraries, which contain files that identify and fix, quarantine or delete viruses.

■ **Set laptops up to automatically get updates,** but that also have the ability to manually get updates, since they are sometimes not on your network and therefore are unable to get the pushed updates.

■ **Involve a qualified infrastructure technology partner** to review your situation and implement solutions so that you can be protected and increase your productivity.

Viruses are here to stay. But the more proactive you are in trying to keep them out of your network, the better chance you'll have to make your company virus-free.

RANDY WEAR (rwear@dspi.com) is president of Decision Systems Plus Inc., a member of the Technology Assurance Group (TAG). DSP provides computer and telephone technology infrastructure sales and support nationwide, to increase client's productivity and profitability.Reach him at (847) 699-9960 or randy@mail.dspi.com.