cost. To these we can now add a third problem — the ability of hackers to use printers to successfully invade your network.

It is especially a problem for those CPA firms that hang on to hardware for year after year. Or, in this case, more than a couple of years.

Researchers at Columbia University have found that printers connected to the Internet could be used to steal data, access secure networks and even cause a fire through deliberate overheating. And if you think your printer is not connected to the Internet, check the "Remote Firmware Update" feature that allows the printer to check for updates without human intervention. It can be used to plant customized firmware in the printer's instruction set.

The scary part of all of this is that it neither theoretical or unknown. It was first demonstrated in 2006 and has been acknowledged by printer manufacturers that include Hewlett Packard. And because the threat resides in the printer, networks based on the Mac and Unix operating systems are not immune. Finally, removing a virus or Trojan once it is inserted into the printer's instruction set would be difficult to impossible.

So do you need to shut off the printer? Not yet. For now, it is possible to establish a first line of defense by making sure your printers were manufactured after 2009. That was the year that manufacturers began to include digital signature instructions in their code sets. Also, it should help if you simply turn off the ability of the printer to access the Internet (or sites on the Internet) directly for updates. Neither of these are a fix, but they should hold you until the printer vendors can release patches to fix the problem.

Connectivity is a zero-sum game. For every benefit we derive from the Internet, there is some potential threat that offsets. As it has been for virtually every new technology

since the dawn of man.