In the first part of this two-part series, we looked at some recent cases of counterfeiting and illegal copying of proprietary software. In this article, I present some practical arguments for fighting illegal copying and list some simple advice for staying out of trouble.

Tolerating illegal copying of software is dangerous for any organization. Such toleration sends a message to employees that other forms of illegality may be acceptable to management; examples of disasters due to such attitudes have included industrial espionage and sabotage against competitors. In addition, tolerating illegality opens a firm to blackmail and to vindictive reporting of crimes by disgruntled or fired employees. Finally, US managers must understand that illegal copying of proprietary software is a violation of 17 USC §506(a). Under 18 USC §3571, making ten or more copies of one or more proprietary programs with a retail value of at least $2,500 within a 180-day period is punishable by up to five years in prison and fines of up to $250,000 for the individuals involved in the software theft.

Some practical guidelines for network managers to avoid hassles from counterfeit software:

- When buying PCs from local dealers, be sure that you obtain all the installation CDs and certificates of authenticity for every software package included on the PC disk.
- If you have any doubts about the authenticity of software you have bought for your organization, contact an anti-piracy hotline. The Software & Information Industry Association (SIIA) has one at 800-388-7478; the Business Software Alliance hotline is 1-888-NO PIRACY (1-888-667-4722).

For good measure, here are some simple suggestions for avoiding problems from unauthorized copies of licensed software within your organization:

- Ensure that corporate policies explicitly forbid copying of proprietary software. No legitimate business can tolerate theft by its employees.
- No employee should ever feel pressured to break the law; provide full information on how to report any such pressures to internal employee-assistance services or, if necessary, to outside law-enforcement agencies.
- Bar installation of unauthorized software of any kind by users onto corporate computers. Company laptops, in particular, should not carry unlicensed copies of the users’ personal selection of software from their home computers.
- Audit all your users’ computers to verify compliance with copyright law.
- If you are unclear on whether a software license allows you to install the product on more than one computer (for example, on a main computer and also on a laptop computer if only one of the systems will be in use at any one time), simply call the software manufacturer to find out.
- Be aware that upgrades to a product do not release previous versions you own for distribution to other computers or to other people. An upgrade is a continuation of a
single license for use, not a new product in addition to your previous versions.

* * *

Anti-Piracy FAQ <http://www.siia.net/piracy/faq/default.asp>

Business Software Alliance (BSA) <http://www.bsa.org/>

Software & Information Industry Association (SIIA) <http://www.siia.net>

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.