
SOFTWARE PIRACY

ENGINEERING CIOs FIND NEW WAYS TO COMBAT UNLICENSED SOFTWARE.

By Joseph C. Panettieri

Most people love a good pirate story. Angelo Privetera isn't one of them.

As chief information officer (CIO) of HDR Inc., Privetera guards the Omaha, Neb.-based engineering firm from pirated and unlicensed software—primarily by using systems management software and clearly defined company guidelines.

Still, patrolling the digital high seas isn't easy. This is the age of tight technology budgets, broadband Internet access and ubiquitous CD-ROM burners (which easily duplicate software). Such fast, free and easy access to software is tempting bait to some employees. With little more than the point-and-click of a mouse, they can download copyrighted code and illegally replicate it across multiple servers, PCs, notebook computers or compact discs.

DEREK LEA



"Software licensing is a real problem in a lot of companies," says Privetera, though he isn't referring to HDR. "There are still many unethical people who feel they should not have to pay for software or music that they can download, and many companies don't have the time or inclination to manage this."

Ignoring a suspected piracy problem isn't wise. Aside from the ethical issues, using unlicensed software can open network security holes, increase long-term technology management costs, tarnish a company's image and trigger customer defections.

Some engineering companies claim ignorance when their employees are caught red-handed with unlicensed or pirated software. But that excuse doesn't hold water. Under federal law, companies can be fined up to \$150,000 for each license infringement, and be held liable for their employees' actions.

Always on Patrol

For many companies, judgment day comes when the Business

"The engineering industry is filled with PC users who demand the latest software, so software makers keep a very close eye on licensing in our market."

—TOM RANDALL,
TRANSYSTEMS CORP.



Software Alliance (BSA) starts fishing around. The BSA is a Washington D.C.-based watchdog group representing the nation's leading software companies, including AutoDesk Inc., Adobe Systems Inc. and Microsoft Corp. Unlike many watchdog organizations, BSA's bite matches its bark. The group has fined at least eight engineering companies more than \$500,000 (combined) since 2001 for using unlicensed software. Individual company fines ranged from \$30,000 to \$163,000.

"The engineering industry is filled with PC users who demand the latest software, so software makers keep a very close eye on licensing in our market," says Tom Randall, vice president of information systems at TranSystems Corp. in Kansas City, Mo. "Most engineering companies have received letters from software companies highlighting the importance of proper licensing."

TranSystems has heeded those warnings. Other engineering companies did not.

Last summer, for example, Speece-Lewis Inc. paid a \$50,000 settlement in a case alleging the use of unlicensed software from Adobe and Bentley Systems Inc. The BSA and local investigators cracked the case in August. "When BSA knocks on your door, it's too late to come clean," asserts Robert Kurger, BSA's vice president of enforcement.

When the fine was announced in August, a Speece-Lewis spokesperson said the Lincoln, Neb.-based company had "implemented a stringent program of computer management...to ensure future compliance with all license agreements."



Under federal law, companies can be fined up to \$150,000 for each license infringement, and be held liable for their employees' actions.

Clearly, the BSA takes its mission seriously. And for good reason: Roughly 25 percent of business software in use in the United States is pirated, the BSA claims.

Such widespread piracy cost the U.S. software industry roughly \$1.8 billion in lost revenue in 2002, according to International Planning and Research Corp. (IPR), a consulting firm in West Chester, Pa. Still, skeptics say the figure is inflated, since many offenders willingly take "free" software but would never otherwise consider purchasing it.

Regardless, one thing is clear: "Free" commercial software can come with a steep price. For starters, unlicensed software often lacks timely security patches, which leaves computers vulnerable to hackers. If an engineering company conducts e-business transactions with its customers, unlicensed software

could leave those customers open to attack as well. Moreover, commercial software companies and legitimate technology integrators won't support engineering firms that run unlicensed software. Translation: If a computer with unlicensed software fails, you're on your own.

Protective Policies

Fortunately, savvy engineering firms have found effective weapons to combat software piracy and keep unlicensed programs off their systems.

An effective plan begins with clearly defined software and computer policies, usually written in a company's employee handbook and posted on its internal network or website. At HDR, for example, no software may be installed on a company computer without approval from a specified technology manager. Moreover, HDR requires all software to be "legally acquired and purchased through the purchasing department," according to the company's employee guidelines.

HDR's purchasing department also requires the technology department to submit written justification for the

purchase, a price quote, the software company's license agreement and the program's intended use. To track such purchases, HDR maintains a central database describing all of the company's software licenses.

Automated Patrols

Of course, written procedures can't block a renegade employee from secretly installing unlicensed software on his own. That's where systems and network management software enter the picture.

Most modern operating systems—including Windows XP, Mac OS X and many flavors of Linux and Unix—now include management capabilities that block users from installing software without permission. Also, many businesses now use systems management software to quickly audit their PCs and ensure that proper licenses are in place.

Auditing software can cost \$10,000 or more for a large company, but free alternatives are cropping up from providers that want to sink software piracy. Microsoft offers a free online tool called the Software Inventory Analyzer, which is available on the company's Software Asset Management website (www.microsoft.com/resources/sam). Using the tool, customers can audit their networked PCs and easily identify which systems, if any, lack the proper software licenses.

Many engineering firms already ride the auditing wave. TranSystems, for example, randomly audits the company's 740 PCs, which are scattered across 26 offices.

And at Terracon Inc. in Lenexa, Kan., asset management software tracks every

"Software licensing is a real problem in a lot of companies. There are still many unethical people who feel they should not have to pay for software or music that they can download, and many companies don't have the time or inclination to manage this."

—ANGELO PRIVETERA,
HDR, INC.



application on 1,200 PCs across 60 office locations. Within the next 12 to 18 months, Terracon also intends to deploy systems management software that prevents employees from installing rogue programs on their PCs, according to CIO Frank Milano.

Keeping Afloat

Network auditing and written user policies can go a long way toward combating unlicensed software. But business chal-

lenges remain. Many CIOs feel trapped on an endless upgrade cycle; just when every PC and server has proper licenses in place, software companies seemingly launch a major product upgrade, adjust their licensing terms or phase out an older application.

"There are almost as many types of license agreements as there are software products," quips HDR's Privetera. "Each software product has its own peculiar set of requirements—and many are merely a way of squeezing the customer [for more money]. Some vendors don't let you delete the software from one machine and legally install it on another."

What's an engineering firm to do? Read the fine print on all software licenses and don't sign on the bottom line without aggressively negotiating the best deal possible. When in doubt, call another engineering company's CIO to compare software costs and licensing terms. ■

"When BSA knocks on your door, it's too late to come clean."

—ROBERT KURGER,
BUSINESS SOFTWARE
ALLIANCE



PROTECT YOUR FIRM

The Business Software Alliance recommends the following steps to combat corporate software piracy:

- 1. Develop Policies:** Company management should formulate written policies that describe the proper steps for software licensing/software purchases and deployment.
- 2. Communicate Policies:** Employee handbooks and an HR website should clearly communicate all software and technology policies. Employees should be informed of these policies upon joining the company and reminded of these policies at least annually.
- 3. Enforce Policies:** Deploy network and systems management software that audits all computers, halts unapproved software installs and identifies potential applications that lack proper licenses.