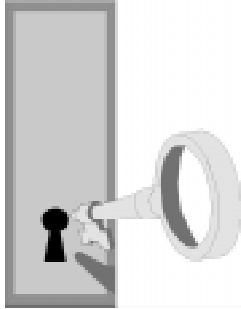


Thursday, Oct. 31, 2002
Vol. 18, No. 23

Soft•letter

BUSINESS INSIGHTS FOR SOFTWARE DEVELOPERS & PUBLISHERS

On Dealing With Software Pirates



How do licensing models, product prices, and copy-protection methods affect piracy rates? See pages 4-6.

The economic impact of software piracy may be hard to measure, but the anger and frustration that piracy inspires can be right off the scale. "People generally do not care," a small developer of training software complained. "We found a \$4 billion company duplicating and distributing our CD-ROM, and it took five phone calls to resolve the problem." Hauling pirates into court is an even more frustrating experience, software developers have found. "We tried – almost begged – for a negotiated settlement," said a CEO whose company got bogged down in a lengthy piracy lawsuit against a client. "The defendants went through the motions, but in retrospect it seems they were just delaying matters."

To prevent these kinds of frustrating encounters, developers and publishers have tried dozens of copy-protection gizmos, dongles, snippets of hidden code, CPU and network locking schemes, encrypted keys, auditing tools – the list sometimes seems to go on forever. And to some extent, technology solutions have been successful: Software these days is significantly harder to steal, and piracy rates do seem to be creeping downward.

But stopping piracy is not purely a technological problem. Often, simple changes in licensing, pricing, support, and marketing can produce a dramatic reduction in piracy rates. There will always be chronic abusers, of course, but (as one developer says) "If we treat people well, they'll generally play by the rules."

What does it mean to "treat people well"? As part of our recent Software Piracy Survey, we asked our readers and friends to share important lessons they've learned about dealing with the software piracy problem in the U.S. (Software piracy overseas is a separate and arguably more difficult challenge.) Their advice reflects a far less adversarial tone than we've heard in earlier piracy discussions; perhaps the software industry and its customers are finally beginning to discover mutual respect:

★ **First, do no harm:** Copy-protection technologies are designed to make life difficult for software pirates, but even the most gentle anti-piracy tools tend to make products harder to use for legal customers as well. "It seems that no matter what you do, someone is going to pirate your software," says Brett Taylor of MicroFour. "The most important lesson is that you should put protections in place, but try not to burden and hinder honest paying clients. These are the people who are paying the bills."

(continued on page 3)

Editor
Jeffrey Tarter
jtarter@softletter.com
617/668-0028

Publisher
Carol Crowell
carolc@ucgtech.com
781/751-8653,
888/400-4768 x253

Associate editor
Sean Edwards
seane@ucgtech.com
781/329-0419 x204

Editorial office
Soft•letter
66 Mt. Auburn Street
Watertown, Mass.
02472
617/668-0028

Subscription office
United Communications
Group
11300 Rockville Pike
#1100
Rockville, Md. 20852
301/287-2718
866/313-0973
customer@softletter.com

www.softletter.com

How to Manage High-Risk Customers

“Getting into a high-profile fight with a customer, even when you’re right, can have a devastating impact on a software company’s reputation,” says business strategist Brian Turchin. “Trouble is, few companies have an early-warning system to spot little problems before they escalate into open warfare. Suddenly, senior management hears that a major client wants to cancel their contract and go to court. And by then it’s usually too late to make peace.”

Turchin, who has managed high-risk software implementation projects and is now writing a book on success strategies, recently shared a few tips on avoiding blow-ups:

- **First, assign a risk ranking:** Every new client project should be identified as “high risk, medium risk, or low risk,” says Turchin. Typical warning signs are too many decision-makers, an excruciatingly long requirements process, obvious internal political conflicts, a history of litigation with vendors, or clueless people on the client’s IT staff. “Most importantly, by talking about risk up front and in the open, you give your staff permission to raise problems as they happen, and not hide them until it’s too late.”
- **Be absolutely clear about who’s doing what:** “This is key, especially on high-risk projects,” he notes. “Vague responsibility assignments invariably cause trouble.” Turchin recommends creating two teams – one, an operational get-it-done group with well-defined milestones and deliverables, and a second executive team that deals with policies and customer relationships. “It’s the particular responsibility of the executive team to scan the horizon and head off trouble,” he says.
- **Document everything:** “Put all agreements, milestones, commitments, and changes in writing. Also, every time your customer holds you up or doesn’t deliver on a commitment, make sure you keep a record. Writing down what was said and done improves clarity and creates a paper trail to use when needed. And with high-risk projects, chances are it will be needed.”
- **Find a high-level friend:** “Establish a trusting relationship with a senior executive from your customer,” Turchin suggests. “Establishing trust from the beginning makes the process of dealing with future problems much easier, since a trusting customer is much more forgiving than an untrusting one.”
- **Don’t compromise on milestones:** Many projects get in trouble because small but critical problems are left to the last minute, Turchin points out. “Programmers are notorious for being 95% complete with a task for weeks on end. Focus on *completion* of milestone deliverables, not on what is partially done.”
- **Be uncomfortable with comfort:** “If a high-risk project is moving along smoothly, it’s easy to become complacent. That’s dangerous. Be skeptical. Encourage your staff to pay attention to those fleeting little uncomfortable thoughts lodged at the back of the brain – and then bring them forward at regular weekly status meetings.”

Brian Turchin, president, Cape Horn Strategies, 2625 Hewlett Ave., Merrick, N.Y. 11566; 516/377-4244.
E-mail: bturchin@capehornstrategies.com.

★ **Educate the customer:** “Corporate end-users are not usually the buyer, so they often don’t understand the terms of software licenses their company has purchased,” John McDonald of Avotus points out. Building in “some form of lock on the software” tends to raise awareness and reduces casual copying, he adds. Other useful reminder techniques include posting license rules conspicuously on a splash screen and in the user manual, and requiring registration numbers for all tech support calls.

★ **Make it easy to be honest:** Complex pricing models and multi-level distribution channels may actually contribute to the piracy problem, some developers argue. “Normally honest users will use illegal copies due to the hassles of trying to purchase more software for their companies,” says John Gilligan of Boothroyd Dewhurst. Ideally, buying additional licenses should be as streamlined as possible. Add-on license pricing should be negotiated up front as part of the basic contract (perhaps with an open purchase order), and users should be able to download additional copies or licenses directly from the Web.

★ **Build an ongoing relationship:** Piracy rates tend to be lowest among users who rely on a software vendor for continuing services, such as maintenance, integration, and custom development. “If customers need service or updates, they’ll pirate for a year or two and then become paying customers,” George Farkas of XBI Software says.

★ **Be human:** “If pirates think they’re stealing from a faceless corporate entity, they won’t feel bad,” Real Software’s Geoff Perlman notes. “When we contact someone we catch copying our software, we always explain that they’re taking money away from *real people*.”

★ **Explore alternative delivery models:** The emergence of remote hosting and usage-based pricing may offer a solution to at least some kinds of piracy. “Our single-user, stand-alone desktop version was the one most likely to get ‘passed around,’” Jim Martin of Inquisite reports. “By moving our single users to a hosted ASP version, this issue has almost disappeared.”

★ **Finally, treat piracy as a marketing opportunity:** Software companies have always handed out demos, trialware versions, student editions, beta test copies, and other giveaways—any configuration that might attract new users. In fact, some of the industry’s most successful software marketing campaigns have relied heavily on distribution of free “evaluation” copies that proliferate throughout whole companies. Once a product is entrenched and has displaced its competitors, marketers point out, corporate buyers are usually willing to sign up for site licenses and maintenance plans. “Don’t worry about stuff you can’t do anything about,” says GraphPad Software’s Harvey Motulsky. “For us, pirated copies are just another form of advertising.”

“The awareness level of license policy issues among enterprise IT professionals is very high due to the efforts of the SIIA and BSA. IT professionals recognize their responsibility to protect their companies legally.”

— Joe Ryan
Funk Software

“The real revenue loss from piracy is low. A dishonest user won’t usually buy a legitimate license if they fail to get the illegitimate one.”

— Nigel Brownjohn
Cyberscience Corp.

“It’s extremely difficult and costly to enforce your agreements. Any efforts above a few phone calls and a letter are usually cost and time prohibitive.”

— Tim Conley
SoftPro Corp.

“Much piracy in our market (high-end servers) is due to mismanagement more than actual intent, at least in the U.S. and European market.”

— Scott Seebass
Xinet

Less Piracy at Higher Price Points

Price of best-selling product or configuration



Percentage of Respondents Reporting "No Known Cases" of Piracy in Past 12 Months (U.S. only)

* Number of respondents by price category: Under 500 = 22; \$500-\$2,500 = 25; \$2,500-\$10,000 = 28; \$10,000-\$25,000 = 20; \$25,000+ = 23.

Benchmarks: Software Piracy Ratios

According to the Business Software Alliance and the Software & Information Industry Association, software publishers are the victims of an epidemic of corporate and consumer piracy. "Forty percent of the world's software is pirated," says the latest BSA piracy study, which claims that the U.S., despite "the lowest rate of any country," suffers from a 25% piracy rate that costs publishers \$1.8 billion a year in lost revenues. In a similar vein, a recent SIIA study concluded (somewhat ambiguously) that 30% of business users "could be classified as pirating software" over the Internet.

But it's fair to ask if this "epidemic" is quite as universal as the BSA and SIIA would have us believe. Clearly, software piracy and outright counterfeiting are a problem in many overseas markets and in segments where high-volume, low-priced titles are easily replicated. For mass-market publishers like Microsoft, Symantec, Intuit, and many game developers, piracy has a serious impact on the bottom line.

For most mainstream business software developers and publishers, however, the problem of illegal copying has far less economic impact—though it's still irritating and costly to fight. That's the primary conclusion that emerges from our latest Software Piracy Survey, which reflects data from 118 companies on their actual and estimated piracy losses in the U.S. market and the methods they use to deal with piracy problems.

Here's what we found:

- **How big is the problem?** For the majority of software companies, piracy in the U.S. has surprisingly little economic impact. In fact, 69% of our respondents report that they experienced "no known cases" of piracy during the past twelve months. Among those companies that did uncover instances of piracy, moreover, actual losses were small, with a median ratio of 1.5 pirated units for every 100 paid units (1.5%).

Piracy Ratios by Licensing Method

	Count	Product Price	No Known Cases	Actual Piracy %	Estimated Piracy %	No Way to Estimate
"Signed contract or purchase order"	44	\$22,500	75%	1%	5%	73%
"Customer must accept license to download or install"	36	\$2,050	60%	1.5%	10%	60%
"Shrink-wrapped license; no customer action required"	34	\$1,500	62%	2%	8%	62%
All respondents	118	\$4,000	69%	1.5%	10%	65%

* Values for Product Price, Actual Piracy %, and Estimated Piracy % are medians. Count is the number of respondents using each licensing method. Four respondents did not specify a licensing method.

To be sure, not all instances of piracy are detected, so we also asked our respondents to *estimate* the total percentage of losses they experience from illegal copying. Even with this approach, we didn't find much evidence of a piracy epidemic: Almost two-thirds of our respondents said they had "no way to estimate" any losses; for those who did make estimates, the median ratio was about 10 pirated units for every 100 sold (10%).

Our data also suggests that piracy has the greatest impact on companies with relatively inexpensive products (see chart on facing page). Below a \$2,500 price point, 45% of software companies experienced a zero piracy rate last year, compared to a piracy-free rate of 86% among companies with products priced above \$25,000. Since lower-cost software typically requires minimal vendor support, greater piracy rates in this segment are probably to be expected; nevertheless, it's significant that even among the most vulnerable companies, almost half uncovered *no* instances of illegal copying in the past twelve months.

- **Does the licensing method make a difference?** Although it's hard to demonstrate a true cause-and-effect relationship between software licensing methods and piracy rates, our survey data (see chart above) indicates that software buyers are most likely to pirate products that are sold with the classic "shrink-wrapped" license, which usually requires no action by the buyer other than opening the box. By comparison, products sold with a signed contract or corporate purchase order tend to have the lowest piracy rates, presumably because buyers must agree in writing to the licensing terms. In fact, even the token agreement embodied in a so-called "click-wrap" license, which requires acknowledgement of license terms before a download or installation can proceed, seems to reduce piracy rates.
- **Does the copy-protection method make a difference?** Software companies have struggled for years to find anti-piracy technologies that stop illegal copying without inconveniencing legitimate users. The most aggressive protection methods, hardware dongles and CPU-locking, do seem to reduce piracy rates—but these methods are also notorious for annoying customers and creating costly support problems.

Piracy Ratios by Copy-Protection or License-Control Method

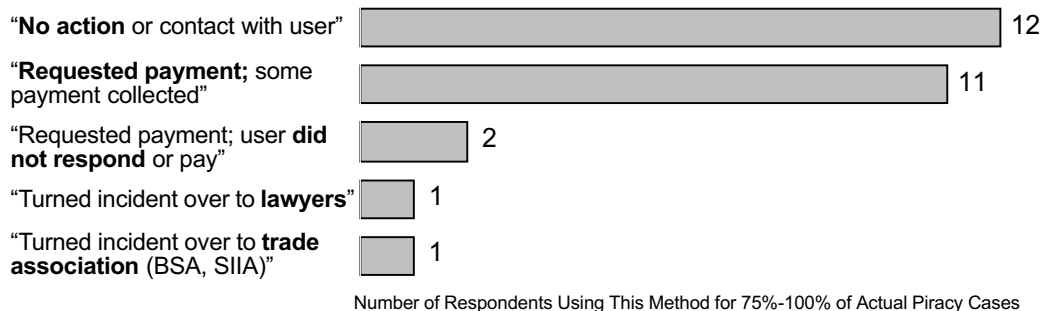
	Count	Product Price	No Known Cases	Actual Piracy %	Estimated Piracy %	No Way to Estimate
"Unique serial number or license key required for installation"	76	\$3,750	60%	1%	5%	59%
" Activation or software locked to CPU"	19	\$3,500	79%	3%	7%	68%
" Network lock or metering"	18	\$6,350	70%	1%	13%	76%
"Hardware dongle "	17	\$5,500	81%	2%	7%	68%
" CD in drive required for product to operate"	6	\$285	n/m	n/m	n/m	n/m
All respondents	118	\$4,000	69%	1.5%	10%	65%

* Values for Product Price, Actual Piracy %, and Estimated Piracy % are medians. Count is the number of respondents using each copy-protection method. Some respondents use multiple methods, so the total of individual methods exceeds the total number of survey respondents. n/m = not meaningful.

Perhaps as a result, by far the most widely used copy-protection method is simply to assign a unique serial number to each licensed user: Almost two-thirds of our respondents say they rely on serialization for protection (sometimes in addition to other methods), and in fact the piracy rate for serialization is actually *lower* than it is for more intrusive methods. To make serialization successful, of course, a publisher has to provide some kind of ongoing service—such as support or free upgrades—that only “legal” users can obtain. But when these services are part of the total product package, they seem to work at least as well as most anti-piracy technology solutions.

- **How do software companies respond to piracy cases?** It’s especially revealing to look at what happens when software companies uncover an instance of piracy (see chart below). The most common response, according to our respondents, is simply to do nothing at all, presumably because the dollars at stake usually aren’t worth chasing. However, many companies do make an effort to contact the offending customer, and they typically manage to collect some payment. Relying on outside legal help for anti-piracy enforcement seems to be the least attractive option; we found only one company that routinely brings in its lawyers to handle piracy cases, and only one company that turns most of its cases over to the BSA or SIIA.

Primary Piracy Response Methods



Behind the Scenes

- PentaSafe Security Technologies:** The multiple reflects the strategic importance to NetIQ, a leader in systems management and Web analytics, of acquiring a comprehensive, best-of-breed security management solution in order to capitalize on the convergence of the two technologies. NetIQ also picks up 1,250 customers, including the Big Four auditing firms. The transaction, which is dilutive but expected to be accretive within 12 months of closing, will provide revenue to offset NetIQ's decline in license fees from Microsoft.
- Prisa Networks:** Information and storage leader EMC, hammered by IT budget cuts and resistance to a proprietary offering, continues its foray into open systems. By acquiring Prisa Networks, a leading supplier of open systems storage area network software, EMC is now positioned to move into the low-end and midrange of the storage systems market. We anticipate additional software acquisitions by EMC, as it seeks to increase its software revenue contribution to 30%, acquire additional open systems market leverage, and use its substantial cash reserve.
- Sparak Financial Systems:** Harland, a leading provider of print and software products to financial institutions, continues to grow its software side. Typical of today's buyer, Harland stays close to home and moves downstream acquiring Sparak, an established leader in integrated hardware and software solutions for community banks. Expect Harland to cross-sell into Sparak's installed base and to boost Sparak's revenues by leveraging Harland's brand and distribution channels. This is an accretive transaction and includes a \$2million earnout, which would take the valuation to 2.0x.
- Campus Pipeline:** SCT, a provider of administrative software to the higher education market, had announced a strategy of providing an e-Education infrastructure platform. Campus Pipeline, serving the same university market, had the products and technology to enable SCT to deliver on the promise. Additionally, Campus Pipeline provides SCT with access to more than 200 colleges and universities. The two companies have had a strategic partnership for more than four years.

Allen Cinzori, Software Equity Group, 12220 El Camino Real, San Diego, Calif. 92130; 858/509-2800. E-mail: acinzori@softwareequity.com. Web: www.softwareequity.com.

Company/Description	Acquired by	Price/Terms	Revenues	Multiple
PentaSafe Security Techs.* • <i>integrated security management solutions</i>	NetIQ Corp. (NTIQ)	\$255,000,000 <i>Terms: Cash & stock</i>	\$36,000,000	7.08
Prisa Networks • <i>storage area network software</i>	EMC Corp. (EMC)	\$20,000,000 <i>Terms: Cash</i>	\$6,000,000**	3.33
Sparak Financial Systems • <i>hardware & software systems for community banks</i>	John H. Harland (JH)	\$32,000,000 <i>Terms: Cash</i>	\$17,000,000	1.88
Campus Pipeline* • <i>software for higher education</i>	SCT (SCTC)	\$27,000,000 ^{EV} <i>Terms: Cash</i>	\$15,000,000**	1.80

* This deal has not closed yet. Terms may change. ** SEG estimate. (EV) Enterprise Value = purchase price plus debt minus cash & equivalents.

Correction: Blue Ocean Software was improperly identified in the 9/15/02 issue. Blue Ocean Software is in the business of IT asset management. Terms of the transaction were cash.



Behind the Scenes is prepared by Software Equity Group LLC, a leading M&A firm serving the software industry exclusively. SEG is solely responsible for its content. This material is based on data obtained from sources we deem to be reliable; it is not guaranteed as to accuracy and does not purport to be complete. This information is not intended to be used as the primary basis of investment decisions.

Beta Testing

- *Beta Testing for Better Software*, by Michael Fine – Excellent overview of beta testing process, with examples; \$40.
- **BetaSphere** (www.betasphere.com) – Beta test management software, outsourcing, tester community.
- **CenterCode** (www.centercode.com) – Beta test management software, outsourcing, tester community.
- **Elementool** (www.elementool.com) – Web-based bug-tracking tool.
- **Beta Test** (betatester.tin.it) – Web site for public beta tests.
- **Beta News** (www.betanews.com) – Web site for public beta tests.
- **Developers Kingdom** (www.developerskingdom.com) – Includes site for public beta tests, primarily for developer tools.
- **Beta Testing License Agreement** (www.weblawresources.com) – Included in Digilaw's Software Agreements template collection; \$60.

SUN MICROSYSTEMS chief executive Scott McNealy on rumors that his board is looking for a replacement: "Good. If anybody wants this job, have at it. It ain't so easy right now. CEOs are the real bums. (Quoted in CRN, 10/14/02)

MULTEX director of investment research Marc Gerstein on the growing number of public technology companies whose market cap is less than the value of the cash on their balance sheets: "It's pretty staggering. It just shows the depth of the market hatred against tech right now." (Quoted in The Wall Street Journal, 10/18/02)

INTRAWEST chief information officer Matthew Dunn on his unhappiness with the complexity of Microsoft's latest "simplified" volume licensing programs: "The most complex code coming out of Microsoft shouldn't be written by the lawyers." (Quoted in Business Week, 10/21/02)

MICROSOFT Office product manager Scott Bishop on his company's new XDoc technology, which lets users embed business processes into documents: "We think XDocs adds the missing link to the Web services story." (Quoted in InfoWorld, 10/14/02)

CENTERBEAM chief technology officer Glenn Ricart on his skepticism about the value of XDocs: "It's assumed there's market demand to build complex, compound documents drawing from various live sources. While that may be the case by the time XDocs reaches market, [so far] the market has expressed little or no desire for this capability since Object Linking and Embedding was introduced five years ago." (Quoted in CRN, 10/14/02)

Soft•letter is published
24 times per year;
entire contents
copyright © 2002 by
Soft•letter.
All rights reserved.
Reproduction by any
means, without
permission of the
publisher, is prohibited.
ISSN: 0882-3499.
Subscription rates:
\$395 worldwide.
Subscription office:
United Communications
Group, 11300 Rockville
Pike, #1100, Rockville,
Md. 20852-3030;
tel 301/287-2718
866/313-0973
customer@softletter.com