

As Seen In

# LOS ANGELES BUSINESS JOURNAL®

LOS ANGELES BUSINESS JOURNAL  
November 2, 1991

## Software Bounty Hunters Cause Trouble for Unsuspecting Firms

**A** lot of people targeted by a software bounty hunter are those who are not even aware they are being targeted. They are the employees of a company who have loaded a copy of a program on their P.C. at work to "do a better job for the boss." And some companies just don't care—they buy one copy of a program and "spread the wealth." If anyone in your company is copying software, you could be looking at thousands of dollars in fines and wasted time repurchasing and auditing programs.

It doesn't matter if you are a software developer or a software user. If you are a software user, you are a target. If you are a software developer, you are a target. If you are a software user, you are a target. If you are a software developer, you are a target.

**SOFTWARE BOUNTY HUNTERS**  
BY GEORGE SAUNDERS

# Software Bounty Hunters Cause Trouble for Unsuspecting Firms

Are you being targeted by a software bounty hunter?

Not sure? Then consider this.

Sometimes a company employee "helps out a friend" by loading a copy of a program into the friend's P.C. at work. Or maybe an employee has a program at home he or she likes, so a copy is loaded into the P.C. at work to "do a better job for the boss." And some companies just don't care—they buy one copy of a program and "spread the wealth." If anyone in your company is copying software, you could be looking at thousands of dollars in fines and wasted time repurchasing and auditing programs.

However innocent or deliberate you or your employees' intentions are, you're just a phone call away from being caught. It could be a disgruntled employee. An irate customer. A vendor with a vengeance. Someday some anonymous tip that you are using unlicensed copies of software could be made to a software bounty hunter and your life will be turned upside down. Just one phone call to a software bounty hunter and you could be branded as a software pirate.

The software bounty hunters are private corporations that have agreements with most software companies who empower them to not only root out offenders but also levy penalties and ensure that the pirated software copies are destroyed. After you've paid your fine, an officer of the offending company is then required to certify that all the pirated software copies have been destroyed. But that's not all. If the value of your unlicensed programs is greater than some threshold set by the bounty hunters, they add your name to a list of "software pirates" that they post on their website and publish at various times to promote their services.

You say you don't want your company to be named on "America's Most Wanted Software Pirates" list? No problem. You pay the bounty hunters an additional "privacy fee" and your name comes off the list. After all, they are bounty hunters.

It's likely that at least half of U.S. companies are pirating some form of software. Office programs like Microsoft® Office, calendar programs such as Sidekick®, and AutoCad®, a computer-aided design program, are just a few of the types of software that get copied and passed around the company at will.

If an anonymous call about pirated software is made directly to a software publisher, they will usually make a deal with the offender to sell them the software license in question at inflated rates. But you're still not safe from the bounty hunters. The software manufacturer may then call the local software bounty hunter and alert them to the fact there may be other pirated programs circulating in your company. The bounty hunter then calls you and threatens to sue for hundreds of thousands of dollars unless you settle with him for something in the neighborhood of 2.5 times the cost of the programs in question. Just how do you prove which of your programs are licensed and which are not? From the bounty hunter's perspective, it's easy. You're guilty until proven innocent. If you bought a program but lost the license certificate, tough luck. That's an unlicensed software copy that will cost you a fine of roughly 2.5 times the cost of the program. That license was an expensive piece of paper you lost.

But guess what—after you pay that penalty to the bounty hunter you still don't own the unlicensed program. You have to go back to the various software publishers and re-buy the original programs. This is because the bounty hunter doesn't sell software. He only enforces piracy claims. Now you've paid about 3.5 times the cost of the program.

So, how do you protect yourself?

1) Don't copy programs indiscriminently!

This is the obvious solution. Do the right thing, pony up and buy the programs your company needs. Don't put your employees in the position of having to do their jobs without the right software tools.

2) Take time to properly store and file your software and your licenses. This comes in handy if you ever do get caught pirating, you can prove which copies are legitimate so you don't get fined for all the copies on your system. Save the original or photocopied licenses in a file (though most people aren't this careful). Or, once the program is installed, return the CD to the original box and put in locked storage so it won't be lost or copied.

3) Purchase a software policing program.

This approach may be best suited for larger companies who sacrifice control to middle managers or employees who work independently. The software costs about \$900 plus \$80 per workstation on your network, but once it's up and running on your mainframe, the program audits the network, monitors activity by terminal and red flags potential piracy.

4) Warn your employees.

Post notices that software piracy is grounds for termination and make good on enforcing your policy.

5) Authorize only one person to install software.

Whether it's your MIS manager or another corporate officer, keep a log of which software is installed on each terminal and who has access to each workstation. Workstations should be password protected.

6) Conduct surprise audits.

Instruct your MIS manager or other corporate officer to take a day or two every year and survey each terminal's hard drive and CD stash for software programs. Armed with an inventory of the licenses you've diligently saved, you'll know exactly how many copies of each program are supposed to be circulating.

7) If you are caught, call your lawyer.

Attorneys experienced in software copyrights can help you identify information that can reduce the amount of the fine. In one recent case, skillful negotiation got the fine reduced by 40%.

Whether it was a corporate decision to steal or your employees are taking matters into their own hands, the business owner is the one responsible for paying the price. Even if you can narrow it down to one rouge employee, you can hold that employee accountable for his actions by firing him. But it's unrealistic to think about suing an employee you've already terminated. Besides—it's too late. Your exposure means it's open season for software bounty hunters and your company might just be what's for dinner. (1059 words)

George Salmas, founder of the Salmas Law Group is an attorney who has spent the majority of his 20-year career in Century City. In 1999, Mr. Salmas was one of three attorneys who tried a trade secret case for Cacique and won a \$24-million dollar trade secret misappropriate judgment. Mr. Salmas also serves as a judge pro tem in the small claims division of the Los Angeles County Courts. Contact him at [GSalmas@Salmas-Law.com](mailto:GSalmas@Salmas-Law.com).

12/01