

## Typology of Software Piracy

Studies of business software usage produce piracy estimates ranging from 40 to 60 %. Piracy rates for home users are much higher. Assuming that losses are random, there is a high likelihood that claims involving a software component entail some form of software piracy. The following typology will assist in the identification of the forms of software piracy that might arise in course of processing a claim for loss.

*Academic Product Leakage:* Software discounted for the educational/academic market segment is illegally sold to people who are not members of an educational institution.

*Change of End User Status:* A user acquires a software package with a licensing agreement that addresses a specific social status, or occupational category. Their social situation changes, but they continue to use the software in violation of their End User Agreement.

*Corporate and Government Under-licensing:* Large corporations, or government departments, install more software than they are legally entitled to under their license agreements.

*Counterfeiting:* Illegal duplication and distribution of “look alike” software products.

*End User Copying:* Unlicensed copying of software by individuals.

*Hard-Disk Loading:* Computer system builders who sell PC's with illicit software preinstalled.

*OEM Unbundling:* OEM (Original Equipment Manufacturer) software is to be sold only with new PC's. Some resellers sell OEM software to consumers separately ('unbundling it') at a lower price, in competition with retail versions.

*Rental:* Users rent and illegally copy software products from a rental store (similar to a video store).

*“Softlifting”:* A small organization purchases one retail copy of software and installs it on multiple computers without paying for the additional licenses.

*Software Piracy on the Internet:* The Internet is becoming the fastest growing means for marketing and distributing pirated software. Over 4,000 sites have been identified for downloading pirated software and there are many others that offer pirated product for sale, fulfilled by CD-ROM media.

Test your understanding of different types of software piracy by trying to match the piracy definitions above with the following claim scenarios:

*Scenario 1:*

The insured installs major productivity applications, borrowed from a colleague, on their notebook computer and then include the face value for the software titles on their Schedule of Loss when the computer is stolen.

*Scenario 2:*

The insured purchases a “clone” system, with illegally acquired software preinstalled, and attempts to make a claim for replacement with legal copies when the hardware is water damaged.

*Scenario 3:*

The insured are carrying on business as retail suppliers of hardware and software. They purchases numerous “counterfeit” copies of a major operating system at a reduced price and suffer a loss due to theft involving a substantial portion of their inventory. They present invoicing in support of their claim for loss that reflects the wholesale cost of legal copies.

*Scenario 4:*

A university student makes a part time business of purchasing discounted “academic” copies of a major office productivity suite and sells several copies, at a profit, to a business that suffers a fire loss wherein the media is destroyed. The insured are unable to replace the media due to their lack of “academic status” and make a claim for loss based on the full retail cost of replacement.

*Scenario 5:*

The insured have 50 installed computers and a 30-user site license for an operating system. They have installed the software on the 20 notebooks used by their sales force alone. A break and enter results in the theft of the laptops and a claim for an additional 20 operating systems.

*Scenario 6:*

The insured have a local area network consisting of a server and six workstations. A single copy of their main database application has been installed on all six workstations and two notebooks. Theft of the workstations results in a claim for replacement of the six copies of the database software at face value.

*Scenario 7:*

The insured are carrying on business as a supplier of custom hardware systems and make a practice of acquiring OEM packages and selling the media and “Certificate of Authenticity” from a single OEM bundle with two separate machines. A fire results in damage to 10 custom systems that were assembled, tested and ready for shipment.

A claim is made for replacement of 20 OEM bundles based on the practice of illegal unbundling of media and documentation.

*Scenario 8:*

The insured is a recent graduate of a graphics arts program and decides to defray the costs of setting up their studio by installing copies of major graphics applications using serial numbers acquired from a “hackers” web site. A destructive virus overwrites the contents of their networked server hard drive resulting in a claim for replacement based on the illegally “hacked” serial numbers.

*Scenario 9:*

The insured acquires and installs a copy of accounting software from a rental outlet. Upon the theft of their notebook computer from a parked vehicle, a claim is made for face value replacement of the installed software based on the legal serial number acquired from the rented software.

*Scenario 10:*

The insured acquires an “educational copy” of a major CAD (computer assisted design) program while attending a community college. Upon graduation, they secure employment but suffer a loss affecting their computer, and software, due to a burglary. A claim is made for the full cost of the current commercial version of the CAD application.