

Beware of the License Police

Software licensing audits are coming your way

By Robert Scott, - Law Technology News
February 2, 2006

Shrinking IT budgets, fierce competition and a mature software market have increased the motivation for software publishers (such as Microsoft Corp., Adobe Systems Inc., Oracle) to conduct software licensing audits -- investigating their customers to determine if they have purchased enough licenses.

Software audits can either be initiated by the software publishers themselves or via their trade associations, such as the Business Software Alliance or the Software and Information Industry Association. Although these groups have no independent regulatory or enforcement authority, publishers have granted them a power of attorney to pursue copyright infringement claims on their behalf.

The most common impetus for a software audit is the report of software piracy received from an informant, usually a disgruntled employee. Companies are not required to cooperate, but avoiding litigation is highly unlikely without an agreement to participate in a voluntary audit.

Think the risk of a software audit targeted at your firm is unlikely? Think again. Gartner, based in Stamford, Conn., estimates that 40 percent of all medium-to-large U.S. businesses will face an external software audit by the end of 2006, and less than 25 percent of public companies have mature software asset management processes. Many experts suggest that private companies are less prepared.

The legal and financial implications of software audits can be enormous. Although software usage is governed by a contractual license, the software industry generally relies upon the stronger protections afforded by the Copyright Act of 1976, which provides stiff penalties for copyright infringement -- up to \$150,000 per violation if the infringement is willful. As a result, even the average infringement has significant legal and financially material implications.

Here's how to protect your firm:

THE DEVIL IS IN THE DETAILS

When faced with an audit, many companies scramble to pull together the essentials, however basic they may be. For example, many companies find they are unable to produce the proofs-of-purchase necessary to show compliance. This significantly complicates the audit process and puts the firm at greater risk of a significant fine.

Another common error: submitting improper documentation in an attempt to demonstrate proof of ownership. Contrary to popular belief, trade associations and publishers only accept dated proofs-of-purchase, with an entity name matching that of the audited company.

For this reason, wise firms avoid purchasing additional licenses in response to a request for an audit, as these purchases will be considered irrelevant. Further, if changes are made to the network following the audit effective date, the auditors may seek sanctions for spoliation of evidence.

DISCOVERY TOOLS

The most common mistake is failure to compile and produce accurate information about the software actually installed on networks. Collecting the data necessary to respond to an audit can be a very complicated, time-consuming and costly process. Companies should resist the urge to conduct the asset-discovery process manually on each computer, because it is time-consuming and

unreliable.

Automated discovery tool selection is critical to the success of the audit program. However, many automated tools produce the results in a format the company cannot interpret. Even worse, many companies use free audit tools provided by the trade associations. These tools, more often than not, inaccurately report the data and fail to exclude information outside the scope of the audit request. Using carefully selected software will not only significantly assist firms in the audit process but the right tools can also be easily integrated into your systems to ensure compliance on an ongoing basis.

SPECIALIZED LEGAL COUNSEL

Companies also err in the audit process by relying on IT staffs to go it alone when responding to audits. Because software license agreements are contracts, IT professionals are often limited in their ability to properly interpret the license agreements and the corresponding copyright laws, without specialized legal assistance. Licensing considerations that require specialized knowledge and expertise include client access licensing, upgrade and downgrade rights and licensing for nonconcurrent laptop use. Further, any automated discovery that is conducted directly by the company or a third-party provider will not be protected by attorney/client and work-product privileges.

Companies are generally advised to cooperate in the pre-litigation audit process, but in a manner that does not compromise their legal position in the event that out-of-court resolution is not possible. In light of the highly specialized issues that arise, un- or under-represented firms generally make a series of common mistakes that jeopardize their legal positions. An IT department must involve legal professionals with specific software audit defense and software compliance expertise.

EVERYDAY BUSINESS PROCESS

The costs associated with software audits, even those that are resolved successfully, are substantial. Businesses that are most prepared will have the greatest success in defending the inevitable software license audit and save money. Accurately compile and record your proofs-of-purchase, consistently monitor networks and build software license compliance into everyday business processes, and you will fare significantly better when auditors come knocking on your door.

Robert Scott is a partner at Scott & Scott, based in Dallas