BEWARE OF THE SOFTWARE LICENSE POLICE

BY ROBERT J. SCOTT

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 – demanding that their customers demonstrate ownership of licenses for all software installed on their computers. 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. 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. Even average, unintentional infringement can have significant legal and financially material implications.

Companies without experience dealing with software publishers and their representatives often make a number of predictable mistakes when faced with demands that they prepare software audit materials. One common error is the submission of improper documentation in an attempt to demonstrate proof of ownership. Software publishers and trade associations typically only accept dated proofs-of-purchase, with an entity name matching that of the audited company. Companies also often respond to audit demands by scrambling to delete unlicensed software and/or purchase licenses to cover any compliance gaps. However, the latter act is ineffective to mitigate any exposure from the audit (auditing entities almost always focus solely on licenses owned as of the date of their letter demanding the audit), while the latter act invites the possibility of sanctions for spoliation of evidence.

However, the most common mistake made by most target companies 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 usually should resist altogether the urge to conduct the asset-discovery process manually on each computer, because it is often inefficient and unreliable. A better choice usually is to use a carefully selected automated discovery tool to assist with the inventory process. However, the free audit tools promoted or provided by the trade associations should be avoided. More often than not, these free tools 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.

Finally, companies often 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 often are 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 non-concurrent 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.

The costs associated with software audits, even those that are resolved successfully, often are substantial. Businesses that are well-prepared in advance will have the greater success in defending the audit and saving money. Therefore, it is important to accurately compile and record proofs-of-purchase for software licenses, to consistently monitor networks, and to build software license compliance into everyday business processes. In doing so, your company will fare significantly better when auditors come knocking on your door.

Robert J. Scott is Managing Partner of Scott & Scott, LLP, and focuses his practice on technology issues including privacy and network security, regulatory compliance, intellectual property, IT transactions, and IT litigation.★