Software Licensing: A Legal, Not Technology Issue

Why your company needs help from a law firm when the BSA comes calling

by Robert J. Scott

The Business Software Alliance is aggressively going after small and mid-size businesses, accusing them of software piracy. Many businesses are already under investigation, and facing potentially steep fines and bad publicity that could hurt their reputation with customers and business partners.

Despite the fact that this is an issue involving software, it's not something that should be handled by the IT department. It is primarily a legal risk management issue. Because of the complexities involved, companies that are under investigation – or concerned about potential exposure – should strongly consider hiring attorneys with extensive experience in software compliance and asset management to conduct the necessary software audits.

Attorneys with experience handling BSA investigations know the intricacies of such investigations, and therefore are best able to advise clients on software licensing and audit issues. There are alternatives to hiring a law firm, such as using internal IT staff or third-party IT vendors, but these options invite unnecessary risks.

IT staffers or other employees most likely will not be familiar with the legal aspects of software licensing, nor have the time and resources to dedicate to the task of auditing hundreds or thousands of machines. Software license agreements can be very complex, and IT professionals – whether they're management or staff – should not be relied upon to interpret legal documents.

IT vendors, while adept at helping companies inventory their existing software licenses, in many cases do not have the legal background or expertise to provide sound advice to corporations. In the event that a company is subject to a lawsuit related to software licensing, IT vendors would not be able to provide guidance or legal representation.

Among the major benefits of hiring attorneys to conduct the software audits is that the results of the audits will be fully protected by the work-product and attorney client privileges. The results cannot be revealed and used against a company in the event of a BSA audit.

Internally prepared and IT vendor audits, on the other hand, are subject to discovery in the event of an audit by the BSA or other software policing organization. The information would not be protected in the same way that it would if an attorney had handled the audit.

In addition to administering software audits that are privileged and confidential, an experienced firm will be able to advise the business regarding software compliance issues, assist the business in procuring software at wholesale prices, and represent the business in any investigation by the BSA.

The threat of investigation is not to be taken lightly. It has become quite common today for companies – large, mid-sized, and small organizations alike – to become targets of the BSA.

Typically, companies will purchase a slew of servers, desktop computers, and mobile devices over a period of several years as demand for information increases. Multiple departments will acquire applications to run on these machines, often without central control and with inconsistent governance regarding software licensing. Sometimes the applications are installed on numerous systems, even though they were purchased for use on one.

Then at some point a letter will arrive from the BSA disclosing that it has received information that the company may have illegally-duplicated proprietary software products installed on its computers. Specifically, the BSA will state, the company may not have the licenses required to support all its copies of Adobe Acrobat, Quattro Pro, Microsoft Excel and Exchange Server, PowerPoint, SQL Server 2000, Windows 2000 Server, and Symantec Norton Antivirus Corporate.

"As you may be aware," the letter will warn, "illegal duplication of copyrighted software violates federal civil and criminal laws. Federal civil penalties allow for the recovery of statutory damages of up to $150,000 per product where the copyright infringement is found to be willful."

The note will go on explain that the BSA takes reports of copyright infringement very seriously,

and will not hesitate to pursue legal remedies. It will offer the company an opportunity to conduct its own internal investigation into the number of unlicensed software products installed on its computers and report the results to the BSA.

At that point, the enterprise will have little choice but to take the BSA's warning seriously. It will also have little choice but to take the organization's advice to audit its systems and pay any appropriate fines to avoid lawsuits.

This scenario – or something very similar to it – is happening ever more frequently as the BSA cracks down on inadequate software licensing and piracy in the workplace. The BSA is an influential organization, made up of some of the leading software publishing companies in the world including Microsoft, Cisco, IBM, Apple, and Adobe.

The group often relies on disgruntled employees and software vendors to instigate investigations into unauthorized software use. The organization collected more than $12 million in fines from underlicensed companies in 2002. Recently, a company in Akron, Ohio, paid out more than $500,000 in one of the largest U.S. settlements ever. Statutory fines can and do reach as high as $150,000 per violation, so senior business and technology executives must take the issue very seriously.

Illegal use of software can happen for a number of reasons. Sometimes companies try to keep costs down by installing programs on more than one workstation to increase access to the application without paying more in licensing fees. At some companies, employees make unauthorized copies of programs and then distribute them to coworkers. Software licensing is so difficult to manage, in fact, that most companies don't even realize they are out of compliance.

That is why it makes sense to consider expert legal advice from a firm that has dealt with the BSA and is familiar with compliance issues. When choosing software compliance counsel, organizations must make sure they select a firm that has both the technology and legal expertise necessary to achieve IT infrastructure goals, while protecting the business against liability.

The process of assessing compliance should include several key elements, including a network review (taking a snapshot of the organization's network to determine how many computer devices are in use); a document review (examining documentary proof of licensing for all software applications in use at the organization); acquisition of missing titles; and implementation of corporate policies and procedures to limit future risk.

The last item is especially noteworthy. It's vital that organizations have in place a formal, up-do-date policy regarding the licensing and use of software by employees. This policy should include specific rules and guidelines regarding the copying and distribution of applications, use of authorized software, and consequences for failure to meet policy requirements.

It is vital to understand that the BSA has no greater rights to information than the software publishers it represents. If the BSA launches an investigation, organizations should consult with attorneys experienced in technology and software compliance to formulate a strategy.

Many companies that are the target of a BSA investigation scramble to buy additional software to become compliant. But this strategy has significant risks. For one thing, if an organization makes changes to its network following the BSA's initial letter, the BSA will seek sanctions for spoliation of evidence in the event that there's a lawsuit.

Becoming compliant is not as simple as conducting a self-audit and procuring the needed licensing. Self-audits should be supervised by skilled attorneys to ensure that the results are confidential and that software in use is legitimate. Even the slightest compliance infractions can result in heavy fines, lots of headaches, and bad publicity.

With thorough planning and sound legal advice, organizations can avoid these significant risks.