COPYRIGHT LAW

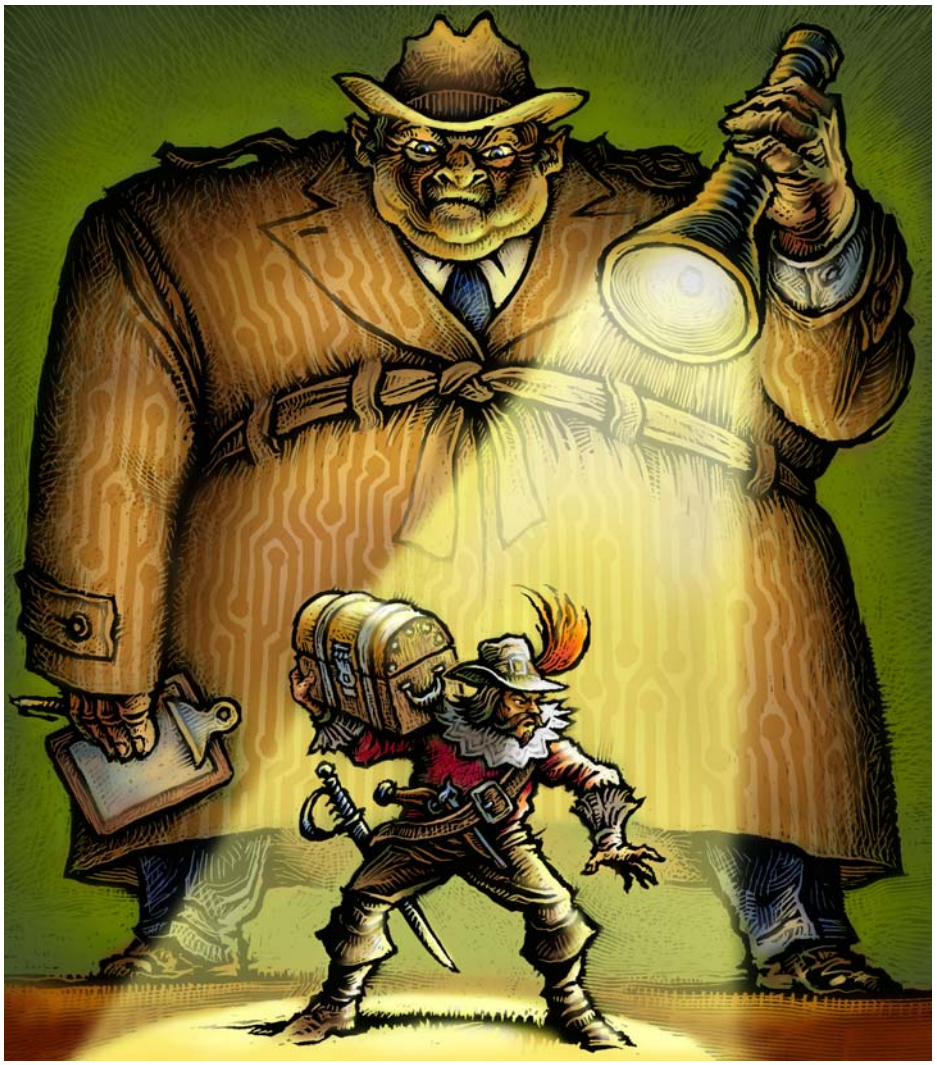
by ROBERT J. SCOTT

Scott & Scott

Surviving Software Audits

How to protect your company when software publishers and their trade groups investigate

ORGANIZATIONS OF ALL SIZES FACE INCREASing threats of legal action by software publishers and their trade associations. Most matters commence with a request for a software audit—a mechanism by which software publishers investigate their customers to determine if they are in compliance with software licenses and copyright laws. In addition to developing internal enforcement operations, many publishers have engaged trade associations to perform enforcement activity under a power of attorney. Industry analyst Gartner estimates that 40 percent of medium to large U.S. businesses will face an external software audit by the end of this year. Businesses



Phil Foster

EXECUTIVE SUMMARY

An increasing number of companies face software audits initiated by software publishers and their trade associations, such as the Business Software Alliance and the Software & Information Industry Association. Many companies are paying substantial fines and suffering negative publicity. Properly preparing for and responding to software audits can reduce the financial and organizational impact on your business. Experienced counsel can help a company properly navigate the audit process and execute proven strategies to protect the company's interests.

that are prepared and properly represented will have the greatest success in defending against the inevitable.

HOW TARGETS ARE CHOSEN

A software audit is initiated by a software publisher or a software trade association such as the Business Software Alliance (BSA) or the Software & Information Industry Association (SIIA). Although the trade associations have no independent regulatory or enforcement authority, software publishers have granted them power to pursue copyright-infringement claims. The most common impetus for an audit is a report of piracy received from an informant, who is usually a disgruntled employee. In some instances, these informants are paid cash rewards tied to the proceeds of the audit.

More often than not, free tools provided by software trade associations fail to exclude information outside the scope of the audit request.

Companies targeted for audit are not required to cooperate with trade associations or publishers, but resolution without litigation is highly unlikely unless the target company agrees to participate in a voluntary audit.

A number of legal issues are implicated in software audits. Although software usage is governed by a contractual license, the software industry generally relies on the stronger protections afforded by the federal Copyright Act of 1976. The act provides stiff penalties for copyright infringement—up to $150,000 per violation if the infringement is willful. Additionally, courts have imposed individual liability on officers and directors of corporations who infringe copyrights, provided they had the ability to control the activity that constituted infringement and that a financial benefit resulted.

Clients generally are advised to cooperate in the prelitigation audit process, but in a manner that does not compromise their legal position in the event out-of-court resolution is not possible. Highly specialized issues arise in these matters, and unrepresented or underrepresented clients often make mistakes that jeopardize their legal position.

LEGAL MISTAKES TO AVOID

The most common mistake we encounter in software audits is the failure to compile and produce accurate installation information. Like many technology projects, collecting the information in response to a request for an audit can be very complicated and time-intensive. At the start of the audit process, the company should select an automated software-discovery tool. Even for small environments, manually reviewing the software on each computer is time consuming and unreliable. Most companies choose an automated process instead.

Selecting the right discovery tool is critical to the success of the audit. Any automated discovery conducted either directly by the client or by a third-party provider will not be protected by the work-product privilege; that privilege applies only to communications between attorneys and their clients. Many tools capture information related to software installations on a computer network, but they produce the results in a format that the company cannot interpret. Even worse, many companies gather the audit information using the free tools provided by the trade associations. These tools, more often than not, inaccurately report the data and fail to exclude information that is outside the scope of the audit request.

Companies also err by relying on their IT staff to respond to the request for an audit. IT employees typically prepare audit reports containing information that is incorrect or beyond what is required to adequately respond. This is particularly problematic because most software audit settlement documents contain a release of liability that is contingent on the accuracy of the results produced during settlement negotiations. If the technology department improperly reports the software installations, the monetary portion of the settlement may be inflated, and the release of liability will be jeopardized.

Another common error is the submission of improper documentation in an attempt to demonstrate proof of ownership for software licenses. Contrary to popular belief, trade associations and publishers accept only dated proofs of purchase—bearing the

EXPERT ADVICE

AUDIT READINESS ASSESSMENT

Are you ready for a software audit? Companies that have effectively mitigated the risks of software audits can answer "yes" to these questions:

- Does your organization conduct routine discovery on 100 percent of its desktops, laptops, and servers?
- Can your organization conduct on short notice a complete reconciliation correlating all installed software to appropriate proofs of purchase?
- Has your organization implemented appropriate electronic controls to prevent unauthorized software-title proliferation?
- Has your organization implemented well-defined processes for retaining and retrieving software licenses and invoice documents?

name of the audited company—as proof that the company owns a license for a particular product. For this reason, companies should avoid purchasing additional licenses of installed software in response to a request for an audit, as these purchases will be irrelevant to the audit. Companies should seek the advice of counsel regarding the purchase of additional software and any impact it might have on the audit and any subsequent litigation that might arise.

OUTSIDE COUNSEL'S ROLE

It is critical to involve experienced counsel in interpreting the software installation data gathered by the automated discovery tool and reconciling it with the available proof-of-purchase information. The installation information should be reviewed to ensure that it includes only information within the scope of the audit.

Additionally, licensing models often depend on the actual use of the product in the company's specific environment. In other words, you cannot interpret the license without a thorough technical understanding of the computing infrastructure and how the software is being used. Specialized knowledge and expertise also are required for considerations including client access licensing, upgrade and downgrade rights, and licensing for nonconcurrent laptop use.

Experienced counsel will be able to provide the audited company with a very accurate estimate of how the auditing entity will interpret the results and the likely monetary aspects of any proposed settlement. Many companies and inexperienced attorneys underestimate their exposure and are unpleasantly surprised by the auditing entity's analysis. Discussing the settlement range in advance helps manage clients' expectations and increases the likelihood of an out-of-court resolution.

To protect the target company's interests, it is advisable to obtain an agreement—prior to producing the audit materials—that Federal Rule of Evidence 408 governs the admissibility of the audit results. Furthermore, the audit materials produced should be narrowly tailored to include only the products identified in the letter requesting a self-audit. The schedules should contain a summary with columns for the product name, cumulative installations, total proofs of purchase, and the excess or deficiency per product. It is also helpful to organize the supporting materials, including the proofs of purchase, by product.

The auditors may refuse to give credit for certain proofs of purchase, or they may seek clarification of the installation information. It is important to review the auditor's analysis critically and provide additional information as necessary. Once the analysis is factually accurate and prior to engaging in monetary negotiations, experienced counsel should make legal challenges to the basis for the proposed fine. A carefully reasoned, legally supported argument will expose the software publishers' weaknesses and increase the chances of a successful result.

NEGOTIATING SETTLEMENT

In trade association audits, the BSA and SIIA include a draft settlement agreement with the opening settlement offer. A number of onerous, nonmonetary provisions should be negotiated prior to settlement. For instance, the BSA often inserts a provision that the BSA can enter and inspect the company's facilities two times per year to ensure that the company is still in compliance with all software licenses. Additionally, the release in the agreement is predicated on the accuracy of the certifications and, in many cases, on future performance of the settlement obligations. Counsel must also carefully advise the client regarding the obligation to certify under penalty of perjury that the company's networks are in compliance as of the settlement date.

Software publishers and their trade associations are targeting companies of all sizes, accusing them of software piracy and copyright infringement. The issues arising in software audits are unique and require both legal and technical expertise. The costs associated with software audits, even when they are resolved successfully, are substantial. Audited companies that enlist experienced counsel to guide them through the process and avoid common mistakes have the greatest chance for the most cost-effective outcome.

Many companies underestimate their exposure and are unpleasantly surprised by the auditing entity's analysis.

ROBERT J. SCOTT is the managing partner of the legal and technology services firm Scott & Scott, LLP. Mr. Scott has extensive experience in software audit defense and advises clients on strategies to reduce the legal, financial, and regulatory risks associated with IT compliance management. He earned his law degree from Hofstra University School of Law, and he is licensed to practice before Texas state courts and numerous federal courts. Mr. Scott is a member of the Dallas Bar Association's Computer Law Section, the IT Compliance Institute, and the Science and Technology Section of the American Bar Association.
rjscott@scottandscottllp.com

"Surviving Software Audits" originally published in the Spring 2006 issue of *8K*.