COMPUTERWORLD
The Voice of the ICT Community

Software audits: not a case of if, but when

Robert J Scott, managing partner of US legal and technology services firm Scott & Scott, gives a lowdown on how to handle software audits

By Kathleen Melymuka, Framingham | Monday, 12 June, 2006

“There are two types of companies: those that have been audited [for software violations] and those that will be.” So says Robert J Scott, managing partner of legal and technology services firm Scott & Scott. Recent settlement fines for software licence violations have topped US $500,000 (NZ$800,000), says Scott, and that’s only a small part of the true cost to an audited company. Scott, who has extensive experience defending companies in software audits, spoke with Computerworld’s Kathleen Melymuka about your rights and responsibilities.

Let’s start with the basics: What is a software audit?

A software audit is a euphemism that describes circumstances under which a publisher or trade association investigates whether its customer is in compliance with software licences and copyright laws pertaining to its products. In many instances, a software audit is conducted under the threat of litigation. They send a letter in which they say they will forgo litigation if you agree to produce proof that you’re in compliance.

Why might I, as a CIO, find myself in the middle of an audit?

There are a number of risks, and the categories depend on the size of the company. If you’re the CIO in a large organisation, you are going to face audits from the vendors directly related to contractual audit rights contained in most software licence agreements. In a mid-size or small businesses, you’re more likely to be targeted by a trade association such as the SIIA [Software & Industry Information Association] or the BSA [Business Software Alliance].

What are the chances of that happening?

It’s inevitable. Adjusted for time, having an audit is a virtual certainty. Most publishers are only enhancing their enforcement operations. Both the BSA and the SIIA have quadrupled the reward money offered to disgruntled employees over the last six months. Most IT budgets are fairly flat, and the only way the industry is going to survive, in their opinion, is by increasing wallet share. One way of doing that is by auditing and using that as a mechanism to generate revenue.

If I’m faced with an audit, how worried should I be?

You should be very worried. A software audit is a big deal for a number of reasons. The biggest is the organisational impact and disruption. There’s also the financial impact, and damage to brand from the negative publicity associated with an unsuccessful audit.

What types of things are auditors from the BSA and SIIA looking for?

The typical request is for the company to document every single installation of software, throughout the enterprise, of the member publishers — what products and how many installations by version — and to produce a dated proof of purchase that demonstrates that the software was purchased prior to the date of the audit letter.

So they want to shift the burden of proof to the company that is the target. It's not, "We'll prove you've done something wrong," but, "To avoid court, you have to prove to us that you haven't done anything wrong."

Think about the impact of documenting every installation of every product, but also the document collection and reconciliation, which is highly time-consuming, expensive and difficult to accomplish.

What are some of the common mistakes a novice IT manager might make when faced with an audit?

The number one mistake people make is to think of this as a purely IT problem. It's not an IT problem solely; it's a legal problem. It's a threatened copyright infringement case, and you need to involve lawyers who have expertise in managing the risks.

Having said that, we have seen clients do things that don't manage those risks. The biggest mistake they make is to go out on an indiscriminate buying spree as a result of receiving the audit letter. But it's too late.

The second-biggest mistake is failure to produce the audit materials as of that effective date. Clients come to us later, and we see that they've presented data that doesn't even purport to be a picture of the situation on the effective date. Typically, it's a picture of the situation a month or so later.

In the meantime, the CEO has gone to the CIO, they've downloaded free discovery tools, they've bought software, they've done a number of things that caused a delay because they haven't been properly advised. And typically, they're not doing the investigation until months later. IT is a dynamic environment; it's constantly changing.

The third mistake is voluntarily producing damaging information to the agencies without securing an appropriate agreement beforehand that they won't use the information against you in court if a settlement is not achieved. We require that any information we give them is limited to settlement discussions, and they cannot take what we give them and use it against us in court.

The fourth mistake is that people fail to understand that there are many monetary and non-monetary components of resolving a software audit as well as post-settlement costs in terms of future audits and certifications, and those post-settlement and non-monetary costs affect the total cost of a software audit.

What steps should a smart IT manager take to prepare for an audit?

The only way to be successful in achieving a low-risk state is to build appropriate processes and procedures into your daily business operations. It needs to be part of procurement, part of IT operations, part of document retention and accounting operations.

You have to comply with good business practices, and implement the tools you need to do internal auditing, so you can constantly manage what you have.

If you don't have in place a programme for software management that can provide internal audits with accurate, predictable and consistent results, you need to get one.