



The Network – Delivers

*Joe doesn't Work Here Anymore;
But he did collect a substantial software piracy whistle
blower reward after he left.*

**Is your software & copyrighted product
asset management process effective?
Are you sure?**

If you do not have a solid IT asset management process & records management process in place, then every time a knowledgeable employee wanders off, you will be at risk. Joe doesn't work here anymore. He left to start his own consulting firm. Good for Joe. Now, where is all the documentation he was supposed to be maintaining? More to the point, did anyone check him out of the company? Or did we just let good old Joe stroll away with no paper trail of his activities in the hardware or software asset management arena?

Joe Didn't Work Alone

What about all the other IT nomads that have blazed through your corporate infrastructure development revolving door? If you think employee, or consultant, or temp worker turnover isn't a problem for IT asset managers, you might want to reconsider from a wider perspective. Visit the members area for a reality orientation that is practically guaranteed to save you money as well as reduce risk.

Former IT Employees

These folks aren't a problem in terms of ongoing operations, right? Not a chance. Let's look at just a few of the problems we tend to overlook when we're up to our eyeballs in day-to-day firefighting.

For the first example, consider one of the more obvious problems we face when we do not have a solid tech asset management process in place. Statistically, former IT employees (and management personnel) who are knowledgeable about your tech environment represent your number one risk of exposure to software & copyright piracy audits.

***“60% of... (software non compliance reports) ...were submitted
by IT staff or managers. More than 75% of reports originated
with individuals who were no longer with the company.”***

SIIA Figures for 2005

Take a Moment & Think This Over

The people who are the most knowledgeable about where you have—shall we call them defects?—in your tech environment are the very ones who tend to report you. Now, quite frankly, if you are intentionally violating copyright, you probably deserve to be confronted. However, and instead, it is much more likely that you are a victim of just plain lousy IT asset management documentation & environment control. You absolutely must establish a formal process for monitoring not only the activities of all technical personnel, but for controlling the copyrighted—or even the expensive—products they use. Otherwise, when—not if—they leave, you may be in for a rude, and expensive awakening.

Unfortunately, Hard Words Work

I am well aware that you do not want to be spoken to in this tone, but I have found that, after over ten years in this business, company management simply does not listen to “nice”. Sugar coating and political correctness have their place, but the unfiltered truth should still gain the most attention. Unfortunately, and sadly (yet questionably), the enforcement industry appears to be correct in their “hit the target hard” attitude: It seems to be the only way to wake people up to the realities represented by license non compliance & piracy. Wounded pride & hurt feelings aside, the only intelligent way to prevent these high cost—high profile—enforcement audit events is to perform systems & software asset management correctly in the first place. Let's go back to Joe's last day and pretend that you have been doing everything right all along.

Joe Knows—But so do You

Throughout Joe's tenure with the company, he has been closely monitored by his direct manager in terms of his systems status reports. Joe has been rigorously keeping & *submitting* closely detailed notes of every support task he initiates or completes on every computer. If he removes software from a system, Joe knows that his report is entered into the asset management repository, effectively placing each uninstalled license back on the shelf for re-distribution or disposal.

Joe also knows that his work is double-checked every day by an automated configuration discovery tool that accurately documents the precise software (and hardware) within each computing device. Joe knows, too, that his daily status report must tally with the discovery tool report. In fact, the asset manager & Joe's direct manager will follow-up with him until all records match. This makes it a bit difficult for Joe to “forget” to document any copyrighted product he may have loaded or un-loaded on any given system.

Finally, from day one on the job, Joe has been made aware that only standardized, company-owned, and fully documented products may be placed on *any* computing

device. What's more, these standards are periodically confirmed with the configuration discovery tool and any violations will, and do, result in punitive actions. Joe is made clearly aware of all policies & procedures relating to copyrighted products and his quarterly evaluation contains both a refresher statement and a formal status update. Joe knows that, if he does not follow policies & procedures, he will be subject to disciplinary action.

You do Things Correctly, Right?

In this scenario, when Joe leaves the company, there should be no credible opportunity for him to release incriminating information to the enforcement industry. If the company asset manager & Joe's manager have followed policies & procedures, this company is clearly performing effective software & copyrighted product compliance assurance practices.

Is there more? Absolutely. But here is a key point: *If* you ensure that the individuals who represent the most significant whistle blower risk are aware of and respect the company policies & procedures, you will have drastically reduced your enterprise exposure to non compliance and piracy audits. *If* effective policies & procedures are in place. *If* they are followed. *If* you ensure that they are being followed and are visible in doing so, you will be ahead of the vast majority of companies in terms of audit exposure. Of course, if you ignore the details, you should probably be concerned.

Consider: Rewards for whistle-blowers are currently ranging from \$10,000 to an incredible \$1,000,000. While these are not equal to the lucrative multi-million dollar executive management separation packages, they are still highly attractive to former employees—both the ethical ones and the ones with an ax to grind. Rule of thumb? If your company tends to generate a large number of disgruntled ex-employees, you might want to get your software & copyright compliance assurance house in order.

At The End of The Day— If you maintain a well-conceived asset management process, establish & enforce policies, and if your company requires that technicians accurately document their work with copyrighted products in a timely manner, you should have no audit worries. Right?

I'm Alan Plastow. Do you want us to follow up on these issues? Let us know. Speak up: Agree? Disagree? Tell us why. Have something to add? Send it in or post it. Want to discuss another subject? Let us know & we'll look into it. Or, as always, feel free to simply kick back & observe.