

“Psst do you want some free software.....???”

TREVOR

by Piper and Lee



The above © copyrighted image used under licence granted to Rob Harmer Consulting Services Pty Ltd ABN 77 053 134 400

If this type of activity is occurring within and across your organization and/or you aren't aware of what is installed or being copied then you are at far bigger risk than you really need to be. Pay attention as we might be able to save your business! The attitude by most to the above cartoon characters is to proceed anyway even if they know it's illegal!

Are you aware that there are reward schemes being offered in Australia (up \$A5,000 and Overseas – Sweden 500,000 kronor, and in the US it recently escalated up to \$US 200,000) that can bring your business down in a screaming heap if you are “reported” for copying and using software in excess of what you have in terms of legally purchased licenses.

Are you aware that if an Anton Pillar order <http://www.pcprofile.com/anton.htm> is served on you that you have 1 hour to have your lawyer present and generally they cannot prevent the seizure and removal from your premises of your computers and assets. Think about how damaging and disruptive this can be for your business. Your client data is now “out of your hands along with other secure commercial and sensitive material”, (this will present a challenge for the Sarbanes Oxley gurus) all through the failure to understand the risks you face due to staff doing the wrong thing by copying software or installing more licenses than the amount purchased. If you thought we were joking when we said there are rewards on offer then check out this link

From time to time industry gurus (Gartner and IDC) will publish annual survey results showing that the software industry is losing \$X billion due to software piracy.

Quite frankly the statistics are really irrelevant to your business. What you need to hear is that your business is losing something in the order of 3 to 5 times that amount due to slack management practises, staff doing the wrong thing, assuming that everything is OK and willingly copying software, music an movies files using your assets. If they are doing the latter then you could be held accountable for aiding and abetting piracy using your corporate assets!

OK so the IT guys in your team will tell you they have it under control, they have audit software and so forth but we can tell you some horror stores over the last 15 years of being and working with businesses and governments to assist them to become more software compliant than what they were before we walked in the door.

Software Compliance Policy

All organizations need a robust software compliance policy that allows them the freedom to operate legally and responsibly under corporate governance rules. This policy, which should have senior management champion and mandate, should ensure that employees share the penalties the organization may suffer if they are caught by one of the many anti-piracy organizations. Sound harsh? Not really.

Organizations must commit themselves to enforcing their software compliance policy. It is no good if it is a "paper tiger"! The software compliance policy should have rules of conduct for installing and using software outlined for both existing and new employees. It should also detail the penalties that will apply if employees are caught using illegal or unauthorized software. "Unauthorized software" covers freeware, shareware, abandonware, demoware, games and other file downloads that are NOT a part of your core business activity! Illegal software covers software that is NOT covered by authorized purchase order for which there is a valid certificate of authenticity AND proof of purchase records that are verifiable and traceable through your accounting system.

Employment agreements, contracts, and letters should include a clause detailing the organization's software compliance rules and how they will be enforced. Without a clear and enforced software compliance policy, employees may think they can install whatever software they like on their PCs. If you are lax in your approach to this then you deserve to feel the brunt of the impact that can follow

While other IT tasks may have a higher priority, software compliance will jump to the forefront if the organization is caught with illegal software. Should that happen, organizations have no option but to defend themselves from a piracy investigation. Many organizations have no idea how to do this and then panic. In many instances, organizations wind up paying large sums of money due to ignorance of their rights, copyright laws and the full extent of the unauthorized software installed (eg; piracy as well as shareware, freeware, spyware) involved in their organization. For that reason, organization's need effective risk-mitigation strategies to minimize the cost of any investigation by police, vendors, or anti-piracy organizations.

Having a software compliance policy is an EFFECTIVE start to the risk mitigation process for your organization!

Management Must Lead with Software Compliance Policies

Software piracy is a people-based problem, so software compliance must combine technology with a management mandate and attention.

Management must change end-user attitudes about the use of illegal and unauthorized software and manage compliance by keeping it focused on the end-user level and holding users accountable.

Moreover, software compliance management should be done in a way that allows the organization and its employees to quickly get on with its core business activities.

Having a robust Software Compliance Policy backed by management mandate can make a difference!

Key Software Compliance Management Tips

For effective Software Compliance Management, keep the following tips in mind:

- Make sure there is a Software Compliance Policy in view at each desktop, on the Intranet, and on the Noticeboard. Add reminders in newsletters from time to time!
- Build software compliance policies into user employment agreements
- Make local management accountable
- Make end users responsible for compliance
- Reinforce desktop compliance policies to limit and minimize software downloading.
- Stamp out the usage of unauthorized/illegal software.
- Send a clear message to desktop users about your software compliance policies and the penalties for violating them.
- Review your policies and procedures Does your company have existing policies outlining software use and acquisition procedures? If so, review them to assure they are still applicable, or, if you have no current policies, now is a good time to write them.
- Implement a software asset management plan
- Once you've worked out the appropriate number of licenses for your software, put a plan in place buy these to make yourself compliant
- Put in a plan to maintain complaint position you have now attained so that the information can be always updated rapidly to reduce your risk.

and finally, **WHEN (Note; not IF, BUT WHEN)** you find out you have illegal software installed;

- If you can identify the staff who have been caught using unauthorized software, ensure staff who are identified as the offenders are given appropriate warnings and/or dismissal if they are known repeat offenders

Don't be frightened to pass on legal costs to clearly identified culprits if the anti-piracy police lay charges and are successful. Share the costs across all offenders!

IN-HOUSE AUDITING IS THE PREFERRED APPROACH

In reality, and in practice, the best personnel to do this task are YOUR OWN TEAM of staff INTERNALLY, once you know how to conduct the audit and the risks involved. Many of these risks can be managed far better internally as you can control them, as long as you take heed of any warning signs that emerge and act promptly.

However, even then, you may be surprised to hear that, in our view, (and in the eyes of many other organizations), software audits (apart from the initial audit) really are a waste of time, money and effort. The tragedy of software compliance auditing thus far is that the initial audit is repeated over and over and over again due to initial failure to complete, interruptions, incorrect data collected, false positive results misleading, lack of identification, failure to match to assets/proof of purchase records and so on.

Wasting money on auditing is no way to run your business entity, when the money for the cost of conducting software compliance audits (in the manner they are being conducted at present) could be far better spent on your core business activities BUT you probably already know this!

Our view, which has been gleaned from many of our customers around the world, since 1991, is that software compliance auditing should;

- be fast,
- be accurate,
- be easy to do,
- be available on demand,
- not involve rocket science,
- not require database/definition file updates,
- not require expensive specialist staff with technical skills,
- not require annual maintenance of up to 25%,
- not deliver false positive results,
- not introduce risk through port scanning,
- be done as little as possible,
- provide un-encrypted results data files,
- not require extensive bandwidth and network resources,
- not slow the network down due to intensive data gathering,
- be done at the absolute minimum cost,
- should only focus on the changes that have occurred between audits,
- make the end -user fully accountable for their actions,
- MUST reduce risk of being caught with illegal software, music and movie titles,

and finally,

- allow the organisation to free up expensive technical and specialist resources so they can focus on issues that are far more important to their business survival i.e. core business activities!

It's as simple as that!

We know that software compliance is NOT the core business activity of your organization and the money spent on traditional auditing techniques is MOSTLY WASTED and could be better deployed and utilized elsewhere.

The most common observation in press releases about Anti-Piracy actions taken, is that the organization " had inadequate procedures in place to prevent the use and installation of unlicensed software..... and "should have had preventative measures in place..... ".

DON'T LET YOUR ORGANIZATION BE QUOTED IN THIS MANNER!

"To combat and overcome both illegal and unauthorized software usage in organizations you need a robust management solution to force a shift in attitude to what is really a PEOPLE based problem!"



For less than 1 hours consultancy fee you can bring over 15 years pc audit experience to utilize in-house without having a consultant set foot inside your door. This might just be the see-change you need to force a change in attitude amongst your staff. See details at http://www.pcprofile.com/SCT_Intranet.htm

PC Audit advice, Software Audit, & License Audit Solutions to overcome - Piracy, Illegal Software, in your organization to reduce risk!

PCProfile

Web site <http://www.pcprofile.com>

e-mail pcprofile@internode.on.net