

Software Compliance Is Not Your Core Business

It's time to take a critical look at software licensing, software audits and audit software tools to find out what we mean by the statement "Software Compliance Is Not Your Core Business".

Three key questions to start the ball rolling

- Is your business making/selling/servicing to make a profit/improve shareholder value?
- Is auditing, monitoring, reconciling and controlling software licenses to stay compliant high on your priority list?
- Why are you in business and what purpose does software play in your success?

When reading this article keep the above three questions in mind as you consider your own position as we are more than certain that the reason you are in business is NOT to conduct software compliance audits but far more productive and profitable activities!

Overview

This whitepaper from PCProfile reflects on how software audits are being conducted at sites as a means to satisfy software compliance requirements and the software audit tools used to perform the task, with a particular focus on the difficulties faced by Small Medium Enterprises (SMEs).

"SMEs carry the greatest software compliance and licensing risk and are often treated as soft targets for enforcement actions due to the way SMEs operate. For an SME the key focus is on their business goals and objectives, and they often lack skills and resources for costly compliance exercises such as Software Asset Management and auditing of software licenses etc." Rob Harmer PCProfile 2008

Although the above statement is pitched at SMEs, what follows applies to some larger organisations as well. The aim of this whitepaper is to help the reader understand more of the issues faced with software licence compliance and auditing of systems.

Running a business is not easy

We all know that, or we should know that. Some of us are cut out for it as leaders, managers or entrepreneurs; others leave the task for others and work as employees for a wage or salary. At the end of the day, the business needs to be successful in its chosen field of play irrespective of whether it makes, sells or provides services, or whether it's a not-for-profit, charity or a government organisation.

There are short, medium and long term goals that are set by stakeholders and targets to be met and achieved and we understand that is the primary focus of the business. Without meeting or exceeding these targets the business venture does not succeed and doesn't have a long life span.

Overlaying the targets set by stakeholders and management, businesses are faced with increasing amounts of regulations and governance from industrial laws, health and safety, environment, corporate governance such as SOX, HIPAA, GLB and a range of state, country and international laws too numerous to mention depending on how far reaching their business trades and operates.

Software compliance is not a regulation but is enforceable through legally binding End User Licensing Agreements (EULAs) issued by software vendors.

A bit of history

Since the 1990's computing has emerged at the desktop level as the most diverse and widespread method of using software tools that enable the user to deliver data and results for the enterprise using software applications that enable the user to calculate, word process, create drawings and images and write content to name a few key processing steps.

Data entry is now taking place at the remotest desktop and hand held devices in lieu of the old centralised processing models used with mainframe systems in the 1960s, 1970s, 1980s and 1990s.

PCs are now so powerful and widespread across business that the processing model has altered significantly since the "centralized" days and of course this has come about due to the proliferation of software applications on the market for a wide variety of tasks and business requirements.

What purpose does software serve in the business?

Software applications at the desktop level really needs to be seen "as a tool to aid the business" in terms of meeting goals and objectives.

Today, enterprises are looking for faster, quicker and more efficient ways of entering the data, assembling the data, summarising and slicing and dicing the data in order to both assess and meet the business goals and objectives.

In simplistic terms software is a "tool in aid" supplied under license (EULA) by each software vendor. Keep this thought in mind as you read on.

Software License Compliance

In holistic terms this means that an organization is fully compliant with the terms and conditions of each EULA in place at the organization.

In simplistic terms (from a pragmatic perspective) it means "one license for each installed application" and this is the line we are assuming in this article.

Let's take a simple example;

If you owned 548 desktop and notebook PCs you would have (using Microsoft Windows as an example) 548 licensed versions installed that could be verified by proof of purchase records.

In a nutshell, that means you have the original invoices from valid vendors that can be used to show supporting evidence that the license count scenario shown above is correct, at all times.

Of course you already know this and you also know exactly how many PCs you have located within your business and how many applications are installed on them. Or are you unsure?

An industry specialist perspective

If you have been keeping an eye on recent exchanges in management circles (see <http://www.channelweb.co.uk/crn/comment/2227890/software-licensing-simplified-4264926> and <http://www.it-director.com/business/compliance/content.php?cid=10747>) there are some industry specialists who have been preaching the mantra that software license compliance is a mandatory issue for consideration at board level due to the risk of being caught with illegal software by anti-piracy police etc

One key aspect of the discussions centres around the need to manage software licenses by continual auditing, monitoring and reconciling licenses to proof of purchase records so as to make sure that your business is complying at all times with software vendor license conditions.

In principle, we don't disagree with the above viewpoint, however in practise we have observed a number of issues which impact and complicate the high moral ground view taken, and when you consider the role of an SME the issues aren't that simple to resolve.

2008 Piracy Study – how relevant is this to you?

You may have seen the 7th Annual Piracy study for 2008 from the BSA and IDC at <http://www.bsa.org/idcstudy> where the commentary is suggesting a forecast drop by a further 10 points in the 4 years 2008 to 2011 “could deliver billions in economic growth and hundreds of thousands of new jobs”. The BSA offers no suggestions or solutions of how they are going to achieve a 10 point reduction in 4 years! For more information on the latest BSA statistics that talk about 10 point rates of reduction in piracy and how much the software industry is losing see [http://www.pcprofile.com/How is the BSA Going To Achieve a 10 point reduction in Piracy Rates.pdf](http://www.pcprofile.com/How_is_the_BSA_Going_To_Achieve_a_10_point_reduction_in_Piracy_Rates.pdf)

From a management perspective, the real issue managers need to realise and face up to is ignore the BSA claims and look seriously at what's happening within their own business area and the costs they are incurring already due to a range of related piracy, anti-piracy and audit areas.

Software licensing models are not simple

Software licensing is today predominantly driven by the needs of each software vendor who often have many and varied licensing and pricing models when you license software for use within a business.

Many of the licences are very complex and the size and structure of the licenses means that many personnel just “accept” them by clicking the Accept button when installing the software, without understanding or even reading the legal terms.

To add to the variety and complexity, are the supplemental license conditions that are issued with patches and fixes. These often vary or replace the original agreement or are to be read in conjunction with the original license agreement, which then affects the original licences issued.

When you spread this across multiple locations in an enterprise there may also be different software versions, different license levels or different stages with software deployments, along with multiple vendors, the task grows to astronomical proportions.

It's no wonder that most organisations today struggle to adequately track and manage software licence usage, and then run the risk of "non-compliance".

Industry "statistics and surveys"

The software industry has banded together into a number of industry groups who are dedicated to concentrating efforts on reducing piracy (not all software vendors are members) and pay an annual membership fee.

One of the outcomes, from these industry groups, such as Business Software Alliance (BSA), along with education and enforcement actions, is a set of annual surveys on the rate of piracy across countries and regions around the world.

The Business Software Alliance who commissioned IDC for the 7th Annual Piracy Study and released the latest results this year shows "industry statistics" that suggests from annual surveys that the levels of software piracy are still unacceptable globally through illegally licensed, under licensed or pirated software.

We are not interested in discussing the method of statistical analysis used, as many other commentators do as they have concerns over the methods use to come up with the numbers.

From time to time, these industry groups engage in enforcement actions resulting from "whistleblower" campaigns, reward schemes and amnesties along with target campaign areas.

Pirates on Parade

After enforcement actions have been underway for a time, the results often hit the press about organizations that have been "caught out" with more software installed than what they had legally paid for in terms of the numbers of PCs deployed across an organization.

Audits by the Business Software Alliance (BSA), or by their agents or third party firms are becoming more frequent, and many that are "caught out" are paraded before the press as being guilty of having the wrong number of licenses installed vs what they could prove they paid for from their record keeping system. Not all the items are published as some settlement actions are under confidentiality agreement not to disclose the parties involved.

The BSA isn't the only organization as there are several variants across countries; eg; FAST, CAAST, SIIA etc

How does this "under licensing" come about?

In reality, few organisations can accurately account for how many PCs and mobile devices they have in their business and when you add to that what software they are running, how much they have paid for it, where it was purchased from and where and how it is used, the complexity increases.

Add to this the ease of which staff can install and load software to your systems (if there are no controls in place to prevent this) then the problem for managers is one of lack of knowledge of what is installed and when the software is mixed with unauthorized software installations, the problem generates huge risk.

Under the duress of a software compliance audit, as happens from time to time (some occur under an Anton Pillar order see <http://www.pcprofile.com/anton.htm>) organizations who have incomplete, inaccurate or are lacking in detail the original information needed to satisfy the audit party, it can be easy to just raise the hands in horror, confess as “guilty” and pay up the sums asked or assessed.

This happens in circumstances when organizations do not have original copies of invoices from software purchases, and even fewer have the details matched to software inventories in a database system!

As a result, when the anti-piracy police ask for proof of purchase matched records to software audits, they often come up short as the data does not exist.

In some cases, because the organization isn't certain whether what they have paid for (assuming they paid for it) is in use, this can lead them to an erroneous conclusion, “that we should pay up, to let us get on with business”.

The end result is usually a public or a private “out of court settlement” which can be a substantial sum of money. Sums quoted in the press on occasions have been of the order of 5, 6 and even 7 figure sums settled “out of court”.

Rule of thumb for settlements

The rule of thumb that we have learnt applies is that the settlement sum that appears in the press is often 1/3rd to 1/4th of the total cost outlay to cover all aspects of the software compliance audit.

The settlement sum usually does not cover;

- the cost of additional licenses to cover the shortfall,
- additional PC equipment to replace equipment seized in an Anton Pillar raid <http://www.pcprofile.com/anton.htm> ,
- costs of legal defence,
- cost of extra staff diverted to be deployed to reconcile and audit, and
- any court fees.

Add to this the loss of productivity and adverse publicity from being “named and shamed” in the press, when caught out.

In addition, managers and owners need to make an undertaking (often in writing and legally binding) not to infringe again and this means an attendant lift in policies and procedures, and training for staff along with increased audit and surveillance, which all comes at a cost.

In some cases a “punish the guilty” stance is undertaken by management and there may be some job losses as a result of failure to adhere to existing procedures and audit regimes.

When you multiply “settlement sums’ appearing in the press by a factor of 3 or 4 times, or even higher depending on the size of the organization, the numbers are quite significant, and this means these costs affects the business cash flow and profits.

Asset Management

Larger organizations in general, are fairly good at managing the “physical” assets although we know of sites that have no idea how many PCs and notebooks they have in the business.

When it comes to software, the area becomes hazy as the software is not usually treated as an asset in the same way that the physical item is, hence the tendency is to overlook sound asset management procedures when it comes to software.

It is known that larger organizations are now investing heavily in centralising license operations, centralising purchasing operations and also adding software asset management solutions that allow for tracking, recording, monitoring and reporting as a means to satisfy software compliance requirements and to reduce their risk from being caught with unlicensed software and to reduce costs of over licensing.

For smaller organizations (SMEs) software asset management systems are not high on the agenda for priority and often they do not have the overhead structure to support internal IT staff or internal audit staff to meet compliance requirements.

Audit tools

There are now a vast array of audit tools available on the market, some free, some suitable for licensing and some are really large enterprise-wide solutions that perform other functions beside auditing such as patch management, software deployment and so on.

Here we are only talking about those tools that either perform a software audit or the software audit functionality portion of a larger asset management enterprise tool.

Some software audit tools require specialist staff with skillsets either acquired through training or from 1st hand experience to use and deploy, especially when it comes to setting up audit control files to detect each application.

Some tools require software identification databases to operate and keep up to date so that latest applications can be detected. Many of the tools use different “detection methods” to identify the software, such as Add/Remove or the Registry and some also generate false positives making the results inaccurate and requiring further validation.

Many audit tools carry the status of a n 800 pound gorilla, are large in size, require installation, extensive training and come with a 180 page or more user manual, requiring significant set up files to enable detection of nominated application packages. To cap that off, they often require updates to software identification libraries to keep up with new software titles released onto the market, and this comes at an annual maintenance fee of between 18% and 25% in some cases.

It's a good time to ask the question - Are you getting value from the significant investment being made in audit tools?

Conducting software audits

Larger organisations are today either self-auditing periodically, or engaging external consultants at high hourly rates, to conduct audits to ensure that software purchasing and licensing policies are being adhered to as a means of reducing risk.

However, for some businesses, auditing, monitoring, reconciling and controlling software licenses to stay compliant is not high on their priority list.

For most SMEs, which are a major proportion of businesses at large, they are not skilled enough or do not have the time and energy and priority drivers to either understand the issues or even tackle the complexities of licensing issues.

The aim of conducting proactive software compliance audits which have been properly reconciled to proof of purchase records with copies of invoices as evidence of proof, is to help organisation reduce its risk and to demonstrate compliance in the event of an external software audit.

Failing to reconcile electronic inventories to invoices from suppliers, ie; conduct the audit alone is not sufficient to offer any protection in any external software compliance audit!

Therefore, if you have been only conducting audits and not taking the next logical step of reconciling to asset and supplier invoices then you are falling short of what you need to verify a compliant state.

Why would you want to match the inventory?

The proof that is required to demonstrate software compliance to an external auditor such as the BSA, is a full inventory with originals of invoices from valid suppliers and this needs to be reconciled and matched to make sure that the counts match and line up.

If you don't have this level of detail, then you are unable to defend yourself in the case of being accused of software "under licensing" ie; more licenses installed than what you have proof you have paid for from a supplier.

It's far better for you to have done this reconciliation process at your own leisure, before the BSA (or another vendor with their lawyers) arrives at your front door as you can reduce your risk if you can ascertain the position beforehand and true up your license position.

Software audits – what really happens

In many sites, software audits are often stopped and started due to other more pressing business imperatives such as server's offline or email systems down. As a result the priority slips as the IT department resorts to fire fighting to keep the enterprise going. In many cases the audits have to be restarted and this is wasted labour, effort and cost and disruptive to business.

Due to the fact that many audit tools deliver false positives, inaccurate results (depending on where they extract data from) and most deliver too much data additional effort needs to be expended in verifying the data results and looking at the enormous amounts of data delivered, sometimes on a daily, weekly or monthly basis depending on the frequency of the audit cycle.

IT staff churn rate affects software audits as well

In terms of software tools, due to the churn rate with IT staff (some are turning over every 12mths to 18mths) the numbers of audit tools that are purchased and never used or used once or twice (with annual maintenance costs of 18% to 25%) due to the personal preferences of the incoming IT manager.

If you changed operating systems on the same personal preference basis each time the IT person changed jobs, you would be filing for Chapter 11 tomorrow as your profit and cash flow is being wasted!

The audit cycle

Some sites have a frequency of audit cycle, depending on the audit tool used, and the skill of the IT person who set it to work, that gathers audit data files on a daily, weekly or monthly basis depending on the audit settings deployed.

In many sites, software audits often need to be stopped and re-started due to other more pressing business imperatives such as server's offline or email systems down.

As a result the priority slips as the IT department resorts to fire fighting to keep the enterprise going.

Where audits have to be restarted this is wasted labour, effort and cost and disruptive to business and does not make it easy to keep a compliant status.

When did you last check that the software audit cycle was completed with all software accounted for, tracked logged, and reconciled to proof of purchase records?

The reality is that software audits are just not a high priority for most sites due to the very intensive and disruptive nature of the activities either before, during or after the audit.

The cost of compliance

In our view, the real issue not being communicated to management at any level, is not how much the software industry is losing, as stated over and over again by annual industry surveys.

Our observations over many years tell us that there are some key cost driver factors that are hidden from management that impact and affect businesses and organization such as;

- the amount of money and effort being wasted by organizations worldwide on buying audit tools (in many cases over and over again),
- using audit tools that are ineffective as they miss key items (through relying on the registry only),
- audit results that are incomplete, due to audits not being completed or restarted,
- inaccurate audit results,
- audit results containing false positives,
- paying somewhere between 18% to 25% annual maintenance for software audit tools,
- updating of software identification database libraries to cover new software releases,
- paying personnel to develop special skills to write script files for audit tools to help identify installed software,
- paying for large teams of personnel as employees (or consultants at hourly rates) to do audits,
- not matching audit results to proof of purchase records to validate "ownership" of licenses,

- paying for more software licenses than what they really need,
- not looking at the impact of movie, sound, image and font files that also contribute to the piracy cost equation and also of downloads affecting network throughput, expanding the size of backup requirements, increase in bandwidth costs and exposing the organization to inappropriate image content (Pornography),
- lost productivity through staff not performing duties they are employed to do, i.e.; not focusing on the organizations' core objectives or business activities.

If you sum up the aggregate of the costs (which affect cash and profit) listed in the bullet points above, you will discover that the numbers are more than likely significantly higher, and yet the rate of piracy is all the BSA is worried about!

The burden of compliance

SMEs carry the greatest risk and are often treated as soft targets for enforcement actions due to the way SMEs operate, focused on their business goals and objectives and lacking in skills and resources for costly compliance exercises such as SAM and auditing of licenses etc.

Now the font vendors are jumping on the bandwagon and showing aggression through enforcing licensing as well and have joined up with the BSA to take actions against font issues and that is an absolute legal minefield! See http://www.pcprofile.com/Font_Piracy_Defend_yourself.pdf and http://www.pcprofile.com/What_The_Font.pdf

Keep an eye out for Font piracy issues as well. If you get served with a summons for Font piracy we advise you engage a technically qualified IT lawyer who can defend you as the jury is out on the real issues of font piracy (unless you set out to steal fonts) as there are significant technical issues that we believe you would be legally entitled to challenge and defend successfully.

In the larger organisations, they have the resources, skillsets and budgets to cover off SAM activities. BUT many companies, particularly the small to mid-sized businesses do not have either, the time, the resources or technical skills to conduct audits etc or cover SAM techniques.

It's the SMEs who are typically treated as soft targets by the software vendors and getting aggressive with SMEs over licensing is not smart at all. Especially when the EULA conditions keep changing over and over again when patches and fixes with supplemental licenses are issued with upgrades. EULAs often have ridiculous clauses in them that make the lawyers happy but do nothing for the business itself.

SMEs do not have the resources necessary to invest in costly compliance programs or SAM despite what vendor solutions are on offer. The focus for an SME is its own business goals and objectives and they would be far better served by a solution offering that allows them to control software themselves rather than be involved in myriad different activation systems, and multiple, sometimes conflicting, EULAs.

Historically, and even more so now in today's economic climate, asset management of software and auditing of systems is NOT high on their priority list of actions to be undertaken, so this makes them a soft target for the ambulance chasing lawyers when it comes to a knock on the door by a software vendor.

The software industry right across the world has failed to offer any solutions to piracy that reduce the burden of compliance for managers of well-meaning but resource-constrained and economically challenged businesses who are now heavily focused on survival.

The onus of compliance currently rests entirely on the end user customer, which are the ones who buy the software from the vendors in the 1st place (in most cases).

Now ask yourself the questions –

- Is your business making/selling/servicing to make a profit/improve shareholder value?
- Is auditing, monitoring, reconciling and controlling software licenses to stay compliant high on your priority list?
- Why are you in business and what purpose does software play in your success?
- What value does software compliance auditing add to the business?
- Why are we in business?
- How can we safely reduce the cost burden of compliance?
- Is there a better way?

Quite Frankly

PCProfile is of the view that you really do have much better things to do than be bothered with the costly burden of software compliance auditing. We already know it is poorly conducted at many sites, and not conducted at all at many others. The compliance burden you face is significant and yet, in our view, the software industry is to blame for the continuation of piracy.

For years the software industry has done NOTHING about offering any solutions to piracy or any solutions to industry to help themselves self regulate and manage the situation.

SMEs carry the greatest risk and are often treated as soft targets for enforcement actions due to the way SMEs operate, focused on their business goals and objectives and lacking in skills and resources for costly compliance exercises such as SAM and auditing of licenses etc.

The software industry is still focusing on solutions to protect their own revenue through activation, DRM, WGA, and lockdown codes, and doing absolutely nothing about assisting any organisation with self regulation and control.

The best the software industry and the anti-piracy bodies can offer is education and punishment through enforcement programs. Our prediction is that software piracy is likely to rise even further in the current downturn in global economic conditions!

The software industry itself is to blame for the piracy issue. It's a bit like selling cars with no speedometer and then being picked on by the police for speeding. Without the control mechanism inbuilt, and visible, who is the guilty party?

Now the font vendors are jumping on the bandwagon and showing aggression through enforcing licensing as well and have joined up with the BSA to take actions against font issues and that is an absolute legal minefield!

In the larger organisations, they have the resources, skillsets and budgets to cover off SAM activities. BUT many companies, particularly the small to mid-sized businesses do not have either, the time, the resources or technical skills to conduct audits etc or cover SAM techniques.

It's the SMEs who are typically treated as soft targets by the software vendors and getting aggressive with SMEs over licensing is not smart at all. Especially when the EULA conditions keep changing over and over again when patches and fixes with supplemental licenses are issued with upgrades. EULAs often have ridiculous clauses in them that make the lawyers happy but do nothing for the business itself.

SMEs do not have the resources necessary to invest in costly compliance programs or SAM despite what vendor solutions are on offer. The focus for an SME is its own business goals and objectives and they would be far better served by a solution offering that allows them to control software themselves rather than be involved in myriad different activation, DRM positions and multiple, sometimes conflicting, EULAs.

Historically, and even more so now in today's economic climate, asset management of software and auditing of systems is NOT high on their priority list of actions to be undertaken, so this makes them a soft target for the ambulance chasing lawyers when it comes to a knock on the door by a software vendor.

The software industry right across the world has failed to offer any solutions to piracy that are to the end benefit of the business side of the equation and also to reduce the burden of compliance for managers of well-meaning but resource-constrained and economically challenged businesses who are now heavily focused on survival.

The onus of compliance currently rests entirely on the end user customer, which are the ones who buy the software from the vendors in the 1st place (in most cases).

“It's time for a sea-change”

It's time for the software industry giants to get their heads together to develop an anti-piracy solution that allows any organisation of any size, small, medium or large, to manage the business through self regulation, by achieving and demonstrating compliance and at the same time reduce costs of expensive SAM solutions, compliance audits and wasting money on teams of auditors and consultants, all of which are an overhead cost to the business.

- *Developing a solution that protects the revenue stream of the software vendor is no longer enough.*
- *Education through enforcement programmes is not enough.*
- *Punishment of SMEs who bear an unrealistic compliance burden is not enough.*
- *Enticing whistleblowers to report pirates through reward schemes is not enough.*
- *Annual surveys talking about a 10 point reduction in piracy rates delivering hundreds of thousands of jobs is not enough.*
- *Forcing through legislation to enforce through Copyright and Free Trade agreements is not enough.*
- *The software industry global giants needs to stand back, take a deep breath and look seriously at simple solution that can be deployed to ease the compliance burden through self regulation.*

The software industry needs to come up with a better mousetrap solution to start making the sea changes needed to overcome the compliance burden issues faced by SMEs and all organizations with controlling and managing software, music and movies as well as fonts! It can be done!

There is a follow-up article that will be released soon that calls on the software industry to get its act together and SOLVE the problem in manner that allows you to manage your business and at the same time reduce the costs of compliance!



Published by PCProfile.com

Worldwide Copyright Notice

Copyright © 2008 PCProfile trading as Rob Harmer Consulting Services Pty Ltd ABN 77 035 134 400 All rights reserved worldwide.

Guidance For Publishers

Publishers are encouraged to publish this report as free content resource in accordance with the following guidelines:

- 1) Articles must be published "as is" (unedited);
- 2) Articles must be published with the author's bio paragraph and copyright information included;
- 3) URLs listed should be set as hyperlinks, with no redirection;
- 4) Whenever possible, authors should be notified of intent to publish;
- 5) This Published Article cannot be used in spam communications or sold;
- 6) PCProfile prohibits the use of copyrighted material in a manner that violates the copyright owner's rights;
- 7) Publishers who violate copyright law are legally liable and subject to possible fines under Copyright Laws worldwide.

Disclaimer

The content of this report is provided for informational purposes only as "guidance notes" and for redistribution as outlined in the "Guidance For Publishers" paragraph and Copyright Notice above. PCProfile does not represent that all technology aspects have been outlined as a complete position and does not accept any responsibility or liability for the use or misuse of the content of this report or reliance by any person of the publisher's contents.

About the Author - PCProfile is an Australian based company located in Adelaide with over 30 years practical computing experience in small, medium and large enterprises and offers managers and business owners in SMEs, and SOHO businesses practical tips and advice on how to get the best out of the technology used by your SME/SOHO business.

An advertisement for PCProfile. It features a man in a white shirt and tie sitting at a desk with a computer, looking stressed with his hand on his forehead. The background is orange and white. Text on the image includes: "Struggling with technology?", "PCProfile offers practical technology tips aimed at helping you use your PC business systems more efficiently.", the PCProfile logo, and the website address www.pcprofile.com.

Struggling with technology?

PCProfile offers practical technology tips aimed at helping you use your PC business systems more efficiently.

PC profile
www.pcprofile.com

Other Self Help "Tips and Tricks" Tutorials and feature articles on management aspects of software piracy etc are available at;
www.pcprofile.com/features.htm

PCProfile also runs seminars on technology topics for SME and SOHO business owners.
www.pcprofile.com email
enquiries@pcprofile.com Mobile 0448 650 227

Seminars www.pcprofile.com/seminars.htm