



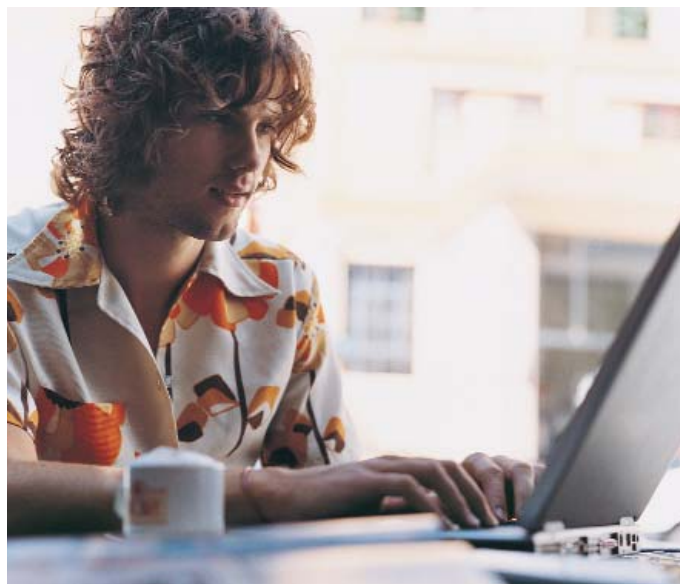
The last decade has seen organizations of all types and sizes investing huge sums in establishing sophisticated computer networks, aimed at enabling employees to better meet customers' needs and create a competitive edge.

Over the same period, the increasing openness of corporate networks (with the introduction of web access, email, and now instant messaging) together with the proliferation of home computing, has led many users to become relatively advanced computer operators.

While this growth in IT sophistication and employee computer-literacy undoubtedly has benefits for the organization, it has also introduced a number of new risks to the corporate network.

The easy access to Internet and email content enjoyed by many employees, coupled with the ease with which software can be introduced directly to computers means that virtually all networks, whether by accident or design, become the resting place for applications and files that they were never intended to play host to.

Left uncontrolled, a potentially vast catalog of unauthorized files and software can quickly accumulate. While on the surface, the dangers associated with these rogue inhabitants of the network might seem confined to wasted storage, reduced network bandwidth and diminished employee productivity; the real risks to the organization can be much worse.



The employer's problem

Thanks to the principle of "vicarious liability", an organization is legally responsible for nearly every action performed on (or from) its network by employees. This doctrine can still apply even if the member of staff concerned was not authorized to carry out the action in question.

In plain English this means that organizations and their directors can, in the eyes of the law, be held personally liable for activities they had no direct part in.

This is why many professional risk analysts now regard mis-use of an organization's corporate network as a distinct issue in its own right, requiring specific management attention as part of the overall risk management strategy of the corporation.

While organizations can never hope to effectively guard against every possible mis-use of the corporate network (this is, after all, limited only by the human imagination), it is possible to identify with some accuracy the 'usual suspects' which present the most common threats on the network.

Unlicensed software

Whether through ignorance or deliberate risk-taking, unlicensed software already exists on the vast majority of corporate networks. Some sources suggest up to a quarter of US and UK software could be unlicensed (a figure that rises steeply in Eastern Europe and Asian countries such as Malaysia).

When an organization 'buys software', in reality it enters into an agreement with the vendor to use a certain number of instances of the application. The software itself is not purchased and the copyright remains with the original publisher. To complicate matters further, many licenses are 'bought' for a time-limited period, after which they are no longer valid.

If the organization installs more copies of the software than it has paid for, or continues to use an application beyond the period of the license agreement, then it is in direct violation of copyright and is subject to the full weight of the law.

Which isn't to say that all copyright infringements are deliberate. Unlicensed software can exist on an organization's network for a range of reasons. While in some cases the company may mistakenly believe that it has removed software that in reality it is still using, the most common cause of unauthorized software proliferation is employees acting on their own initiative without the approval of those responsible for purchasing licenses.

This ranges from a one-off copy made by an employee to enable them to work on two machines, to large scale copying where multiple installations are achieved from one disk without the appropriate license fee being paid.

Likewise, organizations can either deliberately or unknowingly become involved in using increasingly-available counterfeit software, which can be difficult to distinguish from the legitimate versions of products supplied by some major software vendors.

Finally, there is an increasing trend for employees to download software direct from the Internet. While many applications obtained from the internet may be perceived as 'free', in reality most of them need to be licensed in much the same way as packaged software bought off-the-shelf.

Getting tough on license abuse

While in the recent past, the threat of legal action has often been thought a hollow one, many software vendors, together with industry watchdogs such as FAST (Federation Against Software Theft) and BSA (Business Software Alliance), are promising a tougher time for offending organizations in 2004 and beyond.

In the UK, FAST has stated its intention to use the Copyright, Designs and Patents Act 1988 to bring criminal prosecutions against organizations suspected of using unlicensed software.

The BSA, which is funded by software vendors including Microsoft, Symantec and Adobe, has already pursued thousands of legal actions. In May 2004 alone, it levied around \$1 million in fines to US organizations found to be in breach of copyright laws.

The BSA even runs a confidential telephone and web based hotline for individuals to report unlicensed software use in their organization, with financial rewards where a recovery is made.

No matter how the problem has arisen, the doctrine of vicarious liability will ensure that the organization is standing in the employees' shoes when the litigation starts. In most cases, organizations caught using unlicensed software will face back-payment license fees at punitive levels together with damages at the discretion of the court.

Where there has been a deliberate attempt to evade payment of a license fee or to use pirate software, the organization and its principals open themselves to the prospect of a criminal prosecution resulting in (at best) heavy fines and even imprisonment.

Coupled with the inevitable reputational damage and subsequent loss of customers, the results of a criminal case can literally put an organization out of business.



Unauthorized file types

Just as there is a plethora of software that can find its way onto the corporate network, so there are many types of file which bring with them varying levels of risk.

Music

The explosion in use of digital music players, whether desktop-based or portable, has led many workplace computers to play host to vast music collections. While the 'risk' associated with a single user downloading a song from his/her own CD to their iPod via the PC may be no more than a couple of megabytes worth of disk space; the moment that music file is then copied or accessed by another user, the organization becomes responsible for a breach of copyright.

An even greater risk is the downloading and sharing of files through a Peer-to-Peer (P2P) software application – where MP3s and alike are shared anonymously across the internet.

In the US, the music industry has already shown itself more than willing to launch legal actions against the P2P service providers and file sharers themselves. Importantly, a number of these cases have also included substantial claims for damages against the owners of networks that tolerated file sharing.

According to reports, MP3 file sharing in Europe now comfortably exceeds that in the US; which is seen as vindication of the decision to litigate so aggressively against all involved. The International Recording Industry Group, which speaks for the music industry, is on record as saying that similar litigation in Europe is now inevitable and is likely to begin in 2004.



Video

While video clips also present a potential copyright risk to the organization, the dangers associated with this type of file are often wider-reaching.

With many clips containing well-meaning, but often misguided, attempts at humor it is often just a matter of minutes before someone is offended by the content. The resulting harassment or discrimination claim (of which there are more and more every year) can be costly not only for the sender of the mail, but also for the organizations who allowed the message to cross their networks.

These file types are also huge consumers of bandwidth, especially if allowed to proliferate in any number - the effects on network efficiency can be dramatic. Finally of course, the existence of these files in any number raises question marks over how employees are choosing to spend their working time.

Effectively Managing the Risks

While the risks outlined above are growing, they are not all 'new'. As such, many organizations already have in place perimeter security solutions designed to stop unwanted files and software entering the corporate network.

A few forward-thinking organizations have even realized that the issue is essentially one of human behavior, leading them to implement employee education programs.

But the fact remains that software renewals will be missed, staff will find ways to download or install unlicensed applications and files to their PCs, and laws will be broken.

The key to staying on the right side of the law then is to know when the organization is using more copies of an application that it has licensed, to spot when unauthorized software is downloaded to a PC and to sniff out the presence of potentially costly music and video files.

Knowing what to do, however, is only half the battle. Finding the means to do it without causing undue cost and disruption to the business is something else altogether.

Taking charge

Historically, the only way organizations have been able to get a corporate-wide picture of the software and data on their networks was to conduct a physical audit of each and every machine. No wonder then that the time and disruptions associated with such an exercise led many companies to forego auditing in favor of less burdensome tasks.

But what if you could automatically search the corporate network for all PCs, software and file types from a single central server?

IT Asset Management solutions, such as Centennial Discovery, enable organizations to create a clear global view of the entire corporate IT estate by automatically finding and auditing all IT assets on the network.

Suddenly, license managers can reconcile the deployed copies of Adobe Acrobat against the number of licenses physically held by the organization; network administrators can spot which laptops are holding the biggest Jimi Hendrix collections and directors can get an accurate picture of their personal legal exposure.

The last exercise alone is often all it takes to secure board approval for an IT discovery project!



No more legwork

Centennial Discovery uses patent-pending technology to automatically find all devices attached to the network. This means that no matter how a PC, Server or laptop is connected to the network (WAN, LAN, VPN, dial-in etc), Centennial Discovery will always find it.

As soon as it is installed on just a single machine, the inventory solution will start searching the network for other devices – including PCs, servers, switches, printers and firewalls – building a current and complete view of the corporate IT estate. Even when Centennial Discovery has found all the machines on the network, it continues to keep a look out for new devices being added, and alerts administrators accordingly.

Having identified a PC, a Centennial Discovery client agent then performs a full audit of the machine, recording everything from the serial number to a complete list of all software executables and file types located on the hard disk. To make it easy for IT managers to visualize where assets reside in the organization, Centennial Discovery will even track the physical location of each device.

Once deployed, a full corporate-wide software and file audit can be achieved without physically leaving the IT department. And you can perform an audit as often as you like; safe in the knowledge that Centennial Discovery's network-friendly design will ensure that network performance remains at optimum levels.



CENTENNIAL
software

Pre-emptive strike

With organizations like the BSA and FAST publicly stating their intent to bring criminal prosecutions against organizations found to be using unlicensed software and the number of tribunals brought against employers for misuse of corporate IT resources on the increase, the case for reducing a company's legal exposure is clear.

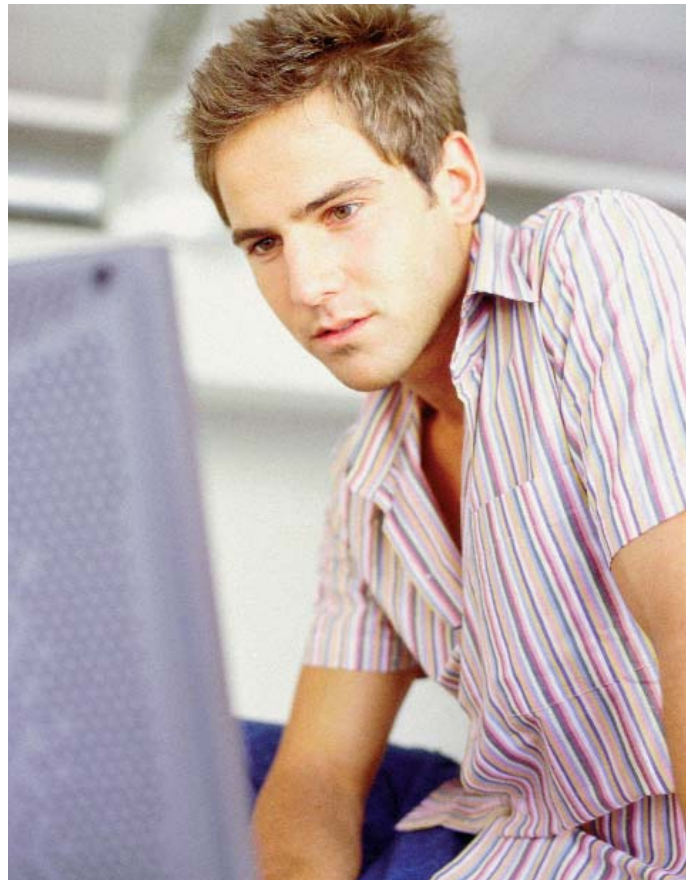
But taking charge of IT use can have clear benefits for the business too. According to analyst firms such as the META Group, an effective IT asset management strategy can reduce an organization's software spend by up to 30% - a significant saving which can undoubtedly be put to good use in other areas of IT.

Surprise yourself

Do you know what's on your network right now? Would you like to know? How about taking a snapshot of just five PCs in your organization?

Download an evaluation copy of Centennial Discovery today and we're sure you'll be surprised at just how much software you find that you never even knew about!

To find out more about how Centennial Discovery can keep your organization in business, visit www.centennial-software.com or contact your IT supplier today.



Vicarious Liability

"An employer is vicariously liable for negligent acts or omissions by his employee in the course of employment whether or not such act or omission was specifically authorized by the employer. To avoid vicarious liability, an employer must demonstrate either that the employee was not negligent in that the employee was reasonably careful or that the employee was acting in his own right rather than on the employer's business."

network discovery & management

www.centennial-software.com