WHEN the internet boomed and content was king, protecting intellectual property became a top priority for online techies, because they knew it was IP that would buy them a Porsche. Clearly such conversations did not reach everyone. The music industry, for example, has provided the IT industry with one of the great cautionary tales of how to ignore a new technology at your peril.

That's why new-media executives rather than record industry executives tend to be more frequent visitors to Porsche sales rooms.

The music industry sat on its hands as the internet arrived in households, and then was left wondering where all its revenue had gone as illegal downloads went through the roof.

The IP protection conversation has now moved beyond the tech community into the business and public sectors.

When Microsoft launched its Windows Rights Management Server platform last year, among its first users was the Australian government's Human Rights and Equal Opportunities Commission.

Its role is to use best-practice systems and processes where they might affect an individual's rights.

Human Rights Department IT services manager Ron McLay says the rights management software effectively adds another layer of security to existing systems and gives the commission better control of documents and email.

Because the commission conducts hearings on some of the most sensitive issues around - race, sex and disability - it added the new information rights capability to better safeguard the privacy of clients.

"We wanted to ensure that nothing would be passed outside the organisation that might have affected the client in any way," McLay says.

Developers took some technologies used in recent years to protect online music and videos and applied them to business.

Software for protecting multimedia content online are known as digital rights management systems and cover consumer products such as music, movies and games.

There is also a whole other world based on corporate IP.

Companies and governments want enterprise-wide systems for protecting intellectual property stored in documents, spreadsheets and the like.

The newer information rights management systems - as corporate IP systems are called - aim simply to only allow authorised access to documents.

It can be also used to protect corporate data from internal users, such as whistleblowers, as well as the thieves, spies and malcontents that the corporate world complains about these days.
IRM is said to have become strangely fascinating to chief executives in corporate America at the time of the Enron/Arthur Andersen scandal. As disgraced chiefs sat perplexed in the dock as supposedly private emails were read to the court, horrified executives watching the show started casting around for better protection.

Billions of dollars have been spent building these IP protection systems, and the technology works. It is also, however, extremely difficult to set up throughout an enterprise, which makes it expensive. A new layer of complexity is added if you want to share information and data with third-party companies as well. Companies invest huge sums to ensure that hackers and other intruders don't access data on their systems - relatively simple stuff.

It's more difficult is to build a system in which each piece of data on the network - from email, to photographs, documents and spreadsheets - has rights management features built in. That means a document can be shared outside the organisation, but the author of the document still controls who is allowed to see it.

The author can specify whether the recipient of the document is allowed to print the document or just view it, and can lock down functions so nothing can be cut and pasted from it.

The author can also put an expiry date on the document so it becomes inaccessible after that period. For chief executives sick of internal documents being leaked to the media, it sounds fabulous.

Enterprise IRM works, but there is a long way to go before it becomes mainstream. It needs network uniformity for a start - software and hardware - and how many large organisations have a uniform network?

It has potential in large organisations, and will probably be used in ways not yet foreseen. S2 Intelligence research director Bruce McCabe says IRM is a natural for the information centres of a range of organisations: government departments, education institutions, corporations, law firms and accounting groups.

"Conceptually it is very interesting, but in practice it will be very hard to do," he says. "If you're adding layers of complexity, you need uniformity, and no-one has uniformity. "Microsoft has been pushing the issues hard, but I think they're pushing it well ahead of what users are designing."

There is a whiff of suspicion that Microsoft is using its IRM strategy as a cloak for a vendor lock-in strategy.

The is nothing like a requirement of network uniformity to keep customers coming back. That's unkind, because IRM is a legitimate software and Microsoft is not the only company making serious investments in its development.

IBM is also keenly pursuing the information rights management market, having also participated in DRM.
Its software strengths reside in the infrastructure layer, and IRM is a logical extension of its products.

The company's electronic media management systems provide rights management services to protect sensitive business data and medical records.

Microsoft launched its rights management services software for Windows last year. It was the first in the industry to unveil a truly mass-market product.

RMS lets large organisations set policies covering who is allowed to view any set of documents, and what they are allowed to do with it once they have it.

The software is designed to staunch the flow of unauthorised information inside or outside an organisation, be it a government department or a multinational company.

In the short term, digital rights management systems will have their biggest effect on email - the favoured conduit of whistleblowers and malcontents when they leak to the fourth estate.

Using Microsoft's RMS system, a manager can define how the email can be used. For example, the manager can restrict the recipient from forwarding the email. Similarly, the manager can restrict: copy-pasting, printing or modification of the email in any way.

An expiry date can be attached to emails after which they can't be opened.

US-based Microsoft security business unit senior director Jon Perera says, with only a hint of a smile, that if the recipient of that email really wanted a copy, they could either take their laptop computer to a Xerox machine and try to photocopy the screen, or get a digital camera and take a photograph.

Either way, it's not a matter of hitting the forward button.

RMS effectively turns any email - or any document attached to it - into a your-eyes-only affair.

RMS is designed to work in conjunction with Office 2003, the new version of Microsoft's desktop applications suite.

The email software within Office 2003, called Outlook, is the most widely used desktop email system on the planet.

Perera says rights management was born out of the company's Windows Media Player and Microsoft Network businesses, where researchers had been doing some "deep thinking" around copyright and intellectual property protection issues involving downloading music and movies.

The term digital rights management has generally been applied to multimedia, and entertainment-related intellectual property.

The newer subset of that research has been information rights management, Perera says. Microsoft took the basic technology and applied it to the corporate workplace, he says.
"As we looked at the technology set, and started speaking to customers, it became clear to us that an early release of digital rights should be made available to customers because it solved a series of pressing business challenges," he says.

"Specifically, customers were saying they needed to share email more secretly, and needed to be able to set up policies."

The issue of rights management - of treating corporate information such as email as an intellectual property asset - has not been widely considered.

Microsoft has not been secretive about its RMS plans, but nor has the product been cranked full of hype in the way a new version of the flagship Windows would be. That does not indicate a lack of interest, though. The company says interest is strongest among large enterprises and governments.

Perera says the technology will find an immediate home in sectors such as health and pharmaceuticals, finance and government.

It is not clear whether any of Microsoft's large local customers, such as the Australian Tax Office, have tested it.

Journalists are wary. Media, Entertainment and Arts Alliance Victorian branch secretary Pat O'Donnell is appalled at the philosophy behind such restrictive mechanisms, let alone the impact the technology would have on journalists.

"Governments obviously want to keep things secret at times, but whether that secrecy is in the public interest is another matter," O'Donnell says.

"It's going to remove any whistleblower from the process, and whistleblowers actually have an important function in our community.

"As communicators, it puts terrible constraints on journalists doing their jobs.

"This is not just about safeguarding documents, it's about removing access to them.

"We're not talking about making confidentiality the exception. This system makes it the rule."

Ironically, much of the momentum that brought the new genre of rights management software to market came from the shocking exposure of corporate largesse that was generated by debacles such as Enron in the US, or HIH and One.Tel in Australia. Such scandals created greater pressure on senior executives and directors to improve corporate governance, measures that encouraged software creators to devise better systems for managing the flow of corporate information.

Wile that meant better record keeping of which people viewed which document at what time, it also meant stopping the leaks.

Microsoft can eat its own dog food. Perera says RMS was first deployed internally 14 months ago - and rolled out to all 56,000 Microsoft staff seven months ago.

Detractors such as O'Donnell say policy restrictions on documents may be disempowering, but Perera says it has been useful in the company, generally among workgroups collaborating on projects.
This report appears on australianIT.com.au.