Information Leakage – the enemy is within

Increasingly, businesses are becoming painfully aware that whilst there are plenty of outsiders who would like to steal some, if not all of their information (people's views as to what is the good stuff vary rather), those with the greatest access, the insiders, are the biggest threat.

This is what is called, rather pleasantly, information leakage. It's a bit like picking up a handful of dry sand. It's difficult to stop it slipping through your fingers. And information leakage is like that, because important information usually comes in little bits, glued together with lots of unimportant information.

Information leakage has been going on for years, sometimes with tacit acceptance by management – mainly because in the paper world you couldn't readily walk out with a lot of information because it was too heavy to carry! Enter the 32 Gigabyte flash drive. That's got enough space on it to hold all the movies you want to see for a while! And if you want to steal a bit more information they will soon come in 1 Terabyte (1,000 GB no less) sizes as well. Fits in your wallet or purse, and holds as much information as a small mainframe computer.

Information leakage has stopped being a nuisance and started to become a menace. In the past the salesmen might take a key customer list with them, or the sales training manual: but now they can take the whole list, trading history, contacts and phone numbers – and still have plenty of room for product documentation, guides, competitive analysis, corporate financial analysis, and even a few interesting emails.

Some of your information has to be protected by the IT people – databases, backup tapes and things like that.

Typically, IT uses encryption in order to prevent the unauthorized from having access to information. But encryption has a major weakness when it comes to information protection. When information has only been encrypted, once it is decrypted the authorized user cannot be prevented from doing whatever they like with the information. In fact, it is totally impossible for the sender of encrypted information to prevent its misuse by the authorized recipient, and quite impossible to ever prove piracy by an authorized recipient. So whilst encryption controls are extremely valuable in some situations, they are not the answer to all the questions.

Further, IT uses access controls to try and protect information for which it is the custodian. Access controls only really work inside the enterprise. Once you get outside the enterprise network it is almost impossible to maintain that control. Further, because access controls were invented back in the mainframe era, they are simple, all or nothing limitations – read, write, append, delete, execute. They have none of the granularity of DRM. If you have access, then it is total and unmanaged.

Also, access controls work at the file level rather than the content level, or at the record level in a database. Neither of these fit the requirement of controlling subsequent use and distribution, which is what DRM is all about (even though it is possible to argue that DRM is nothing more than significantly revised and enhanced access controls).

And what IT can't protect is the information that has to be made accessible to both insiders and outsiders, but is still valuable or confidential – service manuals, competitive analysis, investor guidance, markets analysis, training courses, sales manuals, personal data needed for client meetings and so on.

Also IT can't necessarily protect key internal information such as board minutes, internal briefings, filings with professional advisers, mandatory disclosures and internal research documents. And this is only a short list of the really good stuff that insiders often have ready access to. There are some who say that IT should not have access to this information anyway.

Often important information has to be taken off on laptops or made available to others to see, and then it goes outside of the control of IT anyway. And that is where DRM comes in.

DRM controls provide a continuing control over information that has been distributed, no matter where it is located or what kind of medium it is stored on. DRM controls prevent unlicensed users from having access, even if they can obtain both protected files and licensing information.

That is not to say that security can be total and absolute. If something can be seen on a screen, it can be photographed, and then copied. But DRM controls allow you to add watermarks that identify the authorized user, even on-screen. That doesn't stop copying, but it makes it unattractive to the authorized user to have their name linked to pirate copies, especially these days when prosecutions for illegal game sharing are proving successful as a reality – not merely as a deterrent.

Another essential area of control for DRM is the prevention, or control of printing. In an ideal world printing would be prevented, because any printing means that information can be readily copied. However, if you must allow printing, then you should be able to limit the number of copies that can be made, and provide dynamic watermarking that identifies who the source of the copy is in a way that makes it difficult to remove. Recent successful prosecutions for file sharing in the United Kingdom show that if pirates can be identified they can be prosecuted.

So one of the most effective ways of preventing or significantly reducing information leakage is to implement a DRM control system over the documents containing information that you need to control.

A DRM control system should make it easy for you to protect relevant documents, and simple (preferably transparent) to license regular users of controlled information so that your administration effort is reduced as much as possible, and the need to involve the IT department also minimized. Finally, a DRM control system should allow you to switch off authorized users at a moment's notice if leaks are discovered, or the responsibilities of authorized users change or laptops are lost or stolen. With those features you should be effectively in control of your information.