



Data Loss Prevention (DLP) using Digital Rights Management (DRM)

What is Data Loss Prevention?

Data Loss Prevention (DLP) is a relatively new term created by the IT security industry to describe the need to prevent confidential internal information from going outside the organization that owns or controls it.

Just to make it easy, it is also described as Data Leak Prevention, Data Loss Protection, Information Leak Detection and Prevention, Information Leak Prevention, Content Monitoring and Filtering, and a few more (check with Wikipedia).

As one might guess from all these terms, the basic idea of Data Loss Prevention type systems is to "identify, monitor and protect" by looking at information content and context by filtering and a centralized management system.

The essence of the approach is to try and automate recognizing when content breaks 'the rules' and should be prevented from being sent by email or copied onto a flash drive and so on. So Data Loss Prevention software tries to figure out if the information in a document or spreadsheet is OK or not - and will get it wrong from time-to-time.

But as ever, the devil is in the detail. An enormous amount of 'confidential' information actually has to be shared with third parties - business partners, auditors, government and their agencies, lawyers, staff who do not operate from inside the corporate firewalls. And more - the list goes on.

Data Loss Prevention has boundaries

So whilst some Data Loss Prevention is about stopping the horse getting out of the stable, a whole lot more is needed if you need to do something when the horse is long gone.

And that is where the network monitoring and email scanning skills aren't quite so much help. We have to deal with information that is approved to go outside. So we have to look at how information gets authorized to go outside, and how we stop it 'leaking' once it gets to the recipient.

Relying on the honor system for Data Loss Prevention?

Strangely enough, recipients rarely have an identical view of the need to protect your content, and you need to factor that into your own controls. Much is made of the need to observe an honor code system rather than putting in controls. In an ideal society, honor codes would be all that is needed to protect information, and it is a cheap, efficient measure.

But honor codes have proved a mixed blessing. Michael Collins, writing in the Daily Princetonian on 13 November 2009, noted that, "The distrust of the Honor



Code stems from its history. The Honor Code was written in 1893 as a contract between students and faculty to help prevent cheating. Honor, in those times, meant forcing young white men to follow the rules of older white men. The conservative 19th-century conception of honor has little meaning in an age where students and faculty collaborate." And later in the same article, "The simple reality is that a small segment of students do, and probably always will, cheat. Preventing cheating isn't as simple as locking students in a room."

So apparently honor might not go far enough as an effective Data Loss Prevention solution. And the outsiders have less reason to be honourable than the insiders.

Preventing Data Loss: Encryption fails on its own

The typical answer for a data loss protection system is to encrypt information when sending it to a 'third party' so that unauthorized people cannot 'see' it. But that does not stop authorized people from doing anything they like, or unauthorized people who also have access to that content. Once they have decrypted the file it can be manipulated by all the tools that are available, simply because there is nothing to stop them. It's a bit like saying that information sent protected by SSL is secure. Well, it is whilst it is in the part of the communications network using the SSL, but not anywhere else - like on the server of the recipient which is the normal point of attack of the hacker.

The attractions of using DRM as a Data Loss Prevention Tool

DRM, however, goes the extra mile. It provides controls that limit the ability of those outside the firewall to share or pass on controlled information. It can stop them printing it, or watermark it for printing so that it may be possible to identify the actual source of a leak.

If needed, DRM can report when controlled documents are actually used, and the apparent user opening or printing them. It can also provide controls that allow you to shut off access if you have some concern that documents are being misused (and that could mean letting other people see the authorized screen whilst holding their mobile phones).

Conclusion to Data Loss Protection solutions

Of course, the only true secret is one that is never told. But all too often you find you have to share secrets (preliminary sales figures, competitor analysis, personal information, information for the purposes of litigation, pre-merger company valuation, market analyses - the list goes on) because knowledge of them, in the right circumstances, is essential.

And there's the rub. Data Loss Prevention is interesting for controlling the mundane internal information, but it's only one method used. Manual and documentary and physical access methods are used as well.

But where you have to share secrets, DRM is the only tool that can deliver a true Data Loss Prevention system.



About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection for PDF, flash, ebooks, elearning, software, and web based content. We protect information with US Government strength encryption and rights management controls to ensure complete protection against copyright piracy. Use our DRM software to control document use - stop copying, prevent printing, disable print screen, expire content, instantly revoke access to information, and track document usage (views and prints). <http://www.locklizard.com>