Document Security - a guide to securing your documents

Introduction

When we talk about document security we can have many different ideas as to what security is actually wanted or needed, and what it is there to achieve. In this article we will look at the three principal approaches used today, how they rely upon each other and where they differ. The principle approaches are encryption, DRM and collaboration.

Encryption

Underpinning all digital security systems is encryption. If your prospective document security solution does not use this, then forget it because it is just smoke and mirrors. Encryption is the technology that hides documents from those who are not authorized, and verifies that the content the originator created is unchanged.

If you are an authorized recipient of encrypted information you have the ability to do anything you like with that information once you have removed the encryption. That is the Achilles' heel. The recipient of documents that have been encrypted can go on to use them in any way they wish, and to alter them in any way they wish. That does not mean they can pretend that someone else originated them. And that is a valuable protection, provided you can be bothered to look closely at the authenticity of documents you receive. But judging by the number of people taken in by fake messages from financial institutions or amazing offers from Nigeria, maybe looking to see if a document is real is not a top priority.

Encryption therefore is just the building block of document security but has limited controls.

DRM – Digital Rights Management

DRM looks to take care of continuing control(s) over information. Whether it's a song, film or a book, DRM uses and then goes beyond the capabilities of pure encryption in enforcing persistent controls over the ability to use the content. It is used to limit the ability to distribute (Copyright being the right to make copies and distribute!) or to print, or to view.

Historically, DRM has been used when one entity wants to grant access to its information to another entity, but under controlled conditions. This can be for making sure employees cannot take key documents with them if they leave, or that those who have bought a book, or a training course, cannot pass it on to anyone else without the publisher's permission (and, no doubt, a fee).

The combination of digital rights management controls and encryption ensure documents cannot be shared with others, copied, modified or printed. The use of copy and paste and screen grabbing is usually prevented (depending on the vendor).

If you are looking therefore for complete control over your document security then a solution using digital rights management is what you need to purchase.

Collaboration

Collaboration is an important aspect of document security where document modification is required. Often it does not make use of encryption technology, but relies on access control mechanisms to identify who authorized users are, and to link those identities to the input they made to a specific document.

As you can guess, collaboration is really a precursor activity to DRM. The controls for collaboration are focused over making sure corporate administrators can be certain that only authorized persons had access to and could (or did) amend the document, and that it is properly authorized for distribution. The document that is distributed will appear to be a finished item, and none of the internal management matters will be made available to anyone, either internally or externally. The ability to prevent the use of simple cut and paste or screen grabbing is usually not implemented.

Discussion

The important question in document security is, “What are you trying to achieve?”

If you are just sending confidential documents from point-to-point and are confident that the recipient will not share those documents with others then pure encryption is the right tool for you.

If you need to allow document modification and track who has created/amended/authorized the content of a document, then Collaboration is for you.

But if you want to administer the continuing use of document content and ensure documents are not shared with others then you need to pick a DRM solution. Only DRM solutions provide the controls that you need to make sure your documents cannot be misused, either by staff or customers.

Conclusion

You need to be clear what your objectives are for securing documents, otherwise you can find yourself with the wrong kind of solution and wasted investment.