



Why dealing rooms are better implemented through DRM solutions

Business requirements

In any enterprise there is information that has to be kept secret, but must be distributed, and therefore has to be identified with any recipient in the event that it is 'leaked.'

This white paper addresses two examples of this requirement, and shows how to identify solutions that meet business needs. The first example is the control of board of management information, and the second is the control of information exchanged during mergers and acquisitions.

Statement of the actual problem

The critical feature of both of the above scenarios is that highly confidential information has to be made available to people who are not necessarily to be 'trusted' because their personal future is not determined by maintaining the confidentiality of the information they are being granted access to. That is not to be interpreted in a negative fashion. Independent directors are an essential component guaranteeing the governance of an enterprise. Potential purchasers of an enterprise do not want to reveal secrets, unless, perhaps, they are jilted at the altar of acquisition.

So there's the problem in a nutshell. There are many occasions on which you are obliged to share secrets with people who you cannot control, and you are obliged to take such steps as you reasonably can to reduce their ability to cause harm.

Whilst board minutes are only one example of internal documents that need to be strictly controlled on the one hand, and yet have to go outside of the control of the enterprise, they can contain material that, should it become public for any reason, could have a significant impact upon the share price and future status of the business.

In mergers and acquisitions, the stakes are, perhaps, just blindingly obvious. Information disclosed in this process is usually highly confidential, and misusing the knowledge of that information could be anything from commercially sensitive to requiring explanation to the share trading body of the country in which the enterprise is registered. Or to put it another way, inappropriate disclosure could result in people going to gaol (jail, depending on which version of Monopoly you are playing).

Types of solutions

The typical IT based solution relies upon access controls to prevent the unauthorized from gaining access to information. This may be achieved in a number of ways. For users connecting on an internal network it may simply be logon id and password that grants uncontrolled access to everything defined for that user.



Where outsiders have to be given access to information, IT departments create areas on servers, sometimes called rooms or dealing rooms, where information can be stored, and access controlled through the use of one or more specific logon id/password combinations, perhaps also using incoming IP address monitoring as a means of limiting the potential for people to give their logon details to others, thus defeating the access control.

This latter approach also allows a degree of monitoring of user activity through the use of cookies, and it can be made to appear more secure by using the SSL service to encrypt the information being transferred between the ends.

What neither of these IT approaches achieves is the ability to prevent the authorized user from taking copies of information to which they have legitimate access, and passing those copies on to others. They also do not provide any linkage that can identify the source of unauthorized distribution.

An alternative approach, especially for internal systems, could be to use a document collaboration system. These have various controls for describing controlled groups, and it may be possible to allow outsiders to have access by making outsiders appear to be insiders (rather like the IT solutions considered above). What is more problematic about this type of solution is that collaboration systems expect documents to be editable, and that there is some hierarchy of users where some approve documents. Commonly in the business cases described above, information is authorized before it is made available, recipients are not allowed to change anything, and some activities, such as printing, may need to be forbidden, or tightly controlled.

Finally there are DRM based solutions. These have significant benefits over the other solutions described, because they can allow authorized recipients to use information without having to grant them access either to internal networks or to servers. Where access is granted for limited periods of time this can be automated so that access automatically lapses without further administrative effort, or can be switched on and off again as suits the situation. These facilities are significantly different from administering 'dealing rooms.' Finally, DRM solutions have additional features, such as being able to link the authorized user's identity to viewed images and printed images, to dissuade them from sharing information in an inappropriate manner, as well as preventing authorized users from being able to readily pass on copies of controlled information.

Summary

Dealing rooms were developed using the techniques of a central control system administered by IT departments. They achieved considerable success, although they did not prevent their users from being able to obtain copies of documents and pass them on without detection.

DRM solutions for documents provide a better grouping of controls that better control the use of documents, and provide better operational flexibility for those who have to set up and administer the secure distribution of sensitive information.