Information Rights Management

Best Practices for General User

In university, information is shared all the time, between students or between staff members, but also, between students and staff members or even with people outside the university. However, some sensitive data which can be shared within the university laboratories must not leave the campus. According to Gartner, 84% of high cost security incidents are a result of insiders sending confidential material outside of their company[1]. Therefore, protection of data is of paramount importance to avoid an incident of information leakage. This newsletter will present a solution to prevent files leakage: Information Rights Management.

Protection of Data with IRM

Thanks to the proliferation of the Internet, it becomes really easy to share data. Unfortunately, while information has been spread, it is hard to regulate its use and data leakage is more likely to happen.

- **Data Security Issues**

As soon as information is shared with another person, this one also becomes the owner of the file. The new owner can modify it and forward it without asking the writer permission – the latter loses his right. Moreover, it is impossible to recall information; upon the first sharing the usage is open for ever.

For instance, a student can share a project file with another student (in orange in *figure 1*). The latter can simply change the name on the paper and send it as if it was his work. A solution to prevent him from delivering the exact same work to the teacher (in blue in *figure 1*) should be found.

Figure 1 - Appropriation and forwarding

Another example is that a professor wants to share a file only with students from his class but not others. One of his students can still send it to students from another class as soon as he receives the message.

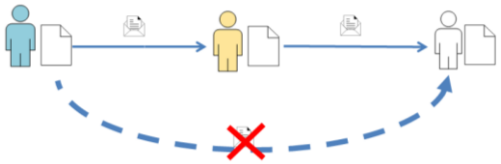

Figure 2 - Unauthorised transfer

Finally, if a file is released outside the institution in which it was created, it will become public and free for everyone. As a result, a lot of information ends up on public websites.

Even in information lifecycle, several steps are sensitive and can threaten data security. Information lifecycle is depicted below[2].

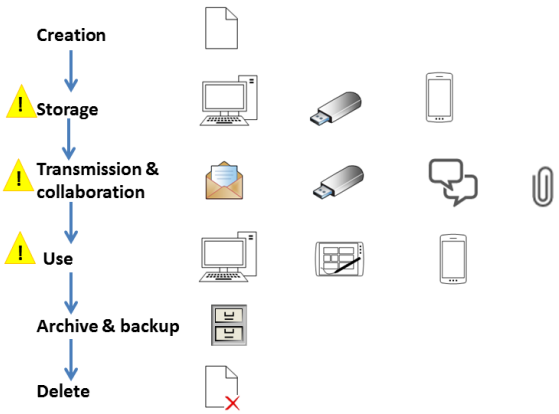

Figure 3 - Information lifecycle

The sign ⚠ indicates the most sensitive steps. In fact, devices for information storage and use can be used for both work and personal purposes which increases data leakage risk. For the transmission step, the multitude of communication channels available increases also the risk.

Therefore, information should be secured all along its lifecycle.

- **Solutions**

In order to protect information during transmission, two options are available:

The first option is *distribution control* (use of external USB drive, Bluetooth, email, etc. are prohibited). This solution will prevent data leakage but will also drastically restrict collaboration.

Another option is *usage control*. Information will be only shared with the right person, at the right time, at the right location and with the right tool. This control of usage is also known as Information Rights Management (IRM)[3]. Corporations will define policies in order to control usage. This will pre-set accessible party, the individual actions authorised (such as reading, printing, forwarding, etc.), temporal and spatial limitations to restrict the access and the location (a specific IP address).

IRM is based on encryption. The decryption key and usage rights can be stored in a database or embedded with the information. The decryption key is valid only for a period of time and thus temporally limiting the use of a file.

- **Benefits**

IRM belongs to the realm of information-centric security which focuses on the security of information rather than on the security of networks, application or data. Unlike other information-centric security, such as data loss prevention and document management system, IRM can be applied even when the information is no longer with the organization. It can embed permissions within files in order to prevent unauthorised modification, printing or pasting of files content.

For instance, a staff member wants to send a file to a certain recipient but does not intend it to be readable to others. Thanks to IRM, if the receiver transfers the file to a third party, the latter will not be able to open it.

Rights can even be modified after the file is distributed. Thus, if a sent file should not be readable anymore, it is possible to remove the reading right even if the file is not in the creator's possession.

Other options are available to reduce access right:

- Snapshots can be restricted on Microsoft platform.
- An availability expiration time can be created to avoid a document access after a certain date.
- During transmission, content exposure can be restricted.

The main advantage of IRM is that it can even protect access to data in motion – data that are not in the organization anymore.

The Practical Usage of IRM

The practical usage of IRM is not difficult; options are generally already implemented in software. However, permission can be delivered only by people who already got them. For example, if someone who only has reading right will not be able to forward the document with writing permission. Thus, only authorised party will be able to implement IRM.

- **Upstream**

Before implementing the system, some crucial points should be identified. Firstly, sensitive contents (documents, email, etc.) need to be defined. Areas where sensitive information is frequently exchanged should be determined. Secondly, to correctly enforce security policies, a list of individuals or groups that are going to use these data and their respective rights (write, read…)

should be established. Other information such as time and period of access or spatial limitation should also be taken into account. Finally, it is crucial to evaluate the consequences of information incident in order to identify the level of sensitivity and thus apply the proper management policy.

- **Document**

Adobe

Sensitive files such as contracts or official documents may require limited access rights. Adobe enables the implementation of IRM on pdf files. Documents can be protected by a password (*Figure 4a*). Document rights can also be specified. A review of document rights and security is available in *Edit* > *Protection* > *Security*.

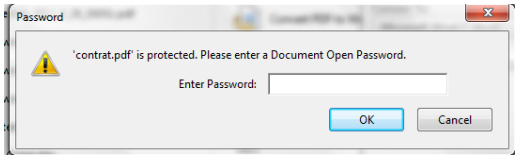

Figure 4a - Password authentication

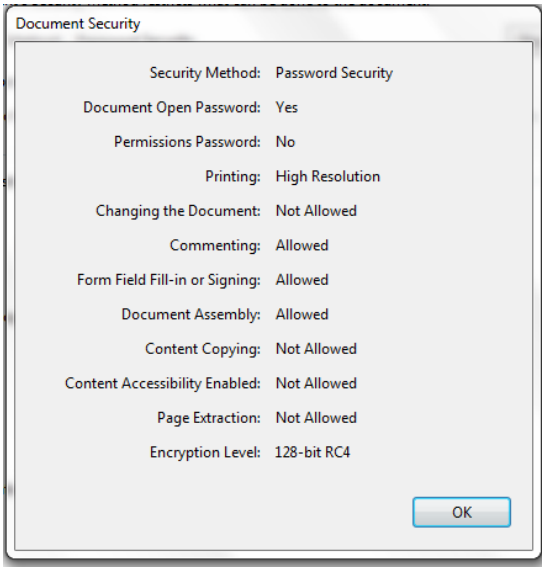

Figure 4b - Security settings

Microsoft

Access can also be restricted by using Microsoft Office (ver. 2010). IRM implementation is enabled on Word, Excel and PowerPoint files. The following paragraph will illustrate the implementation on Word; the process for the other two kinds of files is similar.

For the first use of IRM feature in Office (Word, Excel, PowerPoint and also Outlook), a popup will appear for downloading the updated version of Windows RMS client. Once this has been done, a set of credential has to be prompted. Two kinds of certificates are available: a temporary certificate to test IRM (after its expiration reiteration of the previous step will renew the certificate) or a longer one available in the standard option[4].

In Office 2010 and later version, IRM is included. Once the Word document intended to be protected is open, the following path will lead to an IRM window: *File* tab > *info* > *Protect Document* > restricted permission by *People* > *Restricted access*[5].

After signing up for the free service from Microsoft, another window will appear. This involves the permission setting of the document. However, if the option "*Restricted Permission by People*" is unavailable, the additional module Windows Right Management Services (RMS) Client Service Pack 2 (SP2) will have to be downloaded. The steps to follow are explained in the previous paragraph.

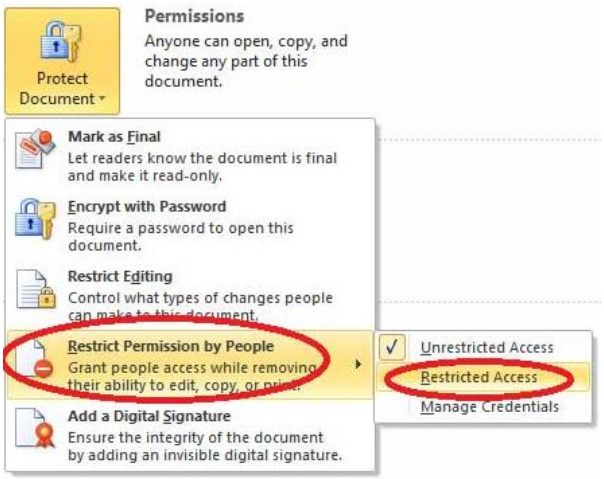

Figure 5 - Word permissions

For documents stored in Office 365, the software Microsoft Azure Right Management has to be used.

- **Email**

Email can also be protected by IRM. Outlook is capable of granting different kinds of permissions such as right to copy, forward, print and define limited period of availability[6].

The permission button which enables accessibility restriction is symbolised by a yellow envelope and a no-entry sign. The recipient will be able to see his restriction status in an info bar. Moreover, an expiration date can be added to the message to prevent the content from being seen after a period of time. An "*Expires after*" check box is available in the "Delivery options".

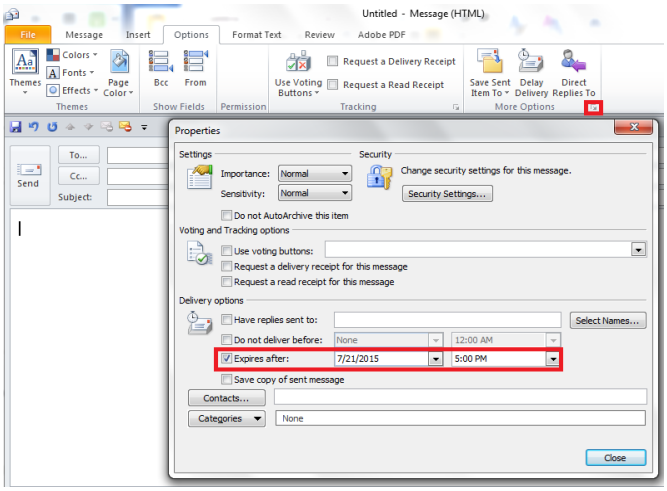

Figure 6 - Expiration settings for Outlook

Permission can also be set for folder access via "*Folder Permission*" in the folder part. Setting permissions for Anonymous will give permissions to everyone. Thanks to this option, people will be able to add and share each other's mailboxes and eventually each other's folders. To do so, the "*Folder Visible*" permission must be enabled and also the checkbox above it. Then, the mailbox should be added in *Tools* > *E-mail Account* > *Next* > *Exchange Service* > *Change* > *More* > tab *Advanced* > *Add*.

Particular rights can be customised. In fact four kinds of permission are available: "*None*", "*Reviewer*", a read-only mode, "*Author*" which enables the creation of items in addition to reading, and "*Editor*" which grants reading, creation and modification rights.

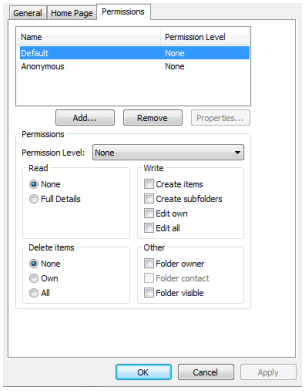

Figure 7 - Folder permission on Outlook

- **Challenges**

The main issue with IRM implementation is a lack of education. In fact, a lot of users have often ignored the need for protecting information, while some IT teams have not acquired in-depth knowledge of IRM technology. Thus, education and training are the keys to ensure the success of IRM.

Digital Right Management

- **Definition**

With the development of the Internet and digitalisation of music, distributing digital content has become more convenient. Digital Right Management (DRM) is designed to prevent common media format from being illegally spread across the Internet[7]. DRM controls access to copyrighted content. For instance, some DVDs cannot be copied for more than two times. DRM ensures that customers will abide by the sharing control set by the owner. In fact, if customers could use media on every devices, they would be allowed to share it with their friends or even to sell it.

Moreover, nobody can know how many times a physical book has been read – whether by its owner or other readers. DRM software can track all those actions. It can also report to the owner or the seller the statistics of the medium or other users activities. Thanks to that, the available time of a medium can be limited according to specific needs and requirements.

- **Differences between IRM and DRM**

IRM is a part of DRM. They both control access, usage and provide right management. Unlike IRM which focuses on the protection of the type of files (email, pdf, word…), DRM protects the content[8]. However, DRM does not entirely resolve the ambiguous question of rights and ownership because each information cannot be separated from the associate rights (update, number of times it can be read…).

The purpose of IRM is to control the access to intellectual property and other confidential information whereas the goal of DRM is to optimise benefits linked to digital contents.

- **DRM in daily life**

Most legal music download services are subject to DRM. In fact, subscriptions are available on these kinds of platforms. For instance, a user can be authorised to download five songs per month after subscription. When the user wants to download a new song, the site has to determine if the quota of download has been reached yet. However, permission is not the only thing the software has to deal with, some rights are also linked to this song. The user may extract a part of the song to use in an audio-mix or the file can be locked. All these rights should be included in the file of the song.

iTunes is also under Apple DRM (FairPlay)[9]. When a song is purchased in the iTunes store, it allows customers to play the song in up to five computers, burn it to CD and play it on unlimited number of Apple devices (iPad, iPhone and iPod). As soon as a song is played on a computer, it generates a unique ID which is sent to the iTunes server to obtain authorization. If the quota of authorization obtained has not been reached, the server will add the new ID to the user's account and send the decryption key to the computer. Therefore, it is easy to learn of the true owner of the song. However, not all devices can play the songs protected by Apple DRM (FairPlay) because of the AAC format (Apple format). Nowadays, new songs purchased on iTunes are DRM-free.

"Fair Use" Issue

If a user downloads an MP3 file which is only allowed to be stored on two authorised devices, and he has made a copy on both a laptop and an MP3 player, later on when he acquires a new laptop, he will not be able to transfer the file from his old laptop to the new one.

The reason is that the system is not able to understand that it is a special case. Only men can judge whether it is a fair exception and exemption from restriction should be granted.

In fact, this can even lead to a trial like the Betamax case[10]. Sony developed in the 70s a video tape recorder: Betamax. Walt Disney Company and Universal Studios sued Sony for copyright infringement. Finally, Sony won the trial on the basis that non-commercial home use recording was considered fair-use.

Conclusion

Universities are recommended to implement IRM in order to prevent data leakage. It is much more secure than shared password and IRM rights can still be modified after information has already been broadcasted.

However, IRM cannot totally protect data rights. In fact, an ill-intentioned person can still retype or take picture of a restricted content. Absolute security does not exist but it is possible to approach.

Education, arousing people's awareness of the danger linked to the publication of unprotected documents, is the key to improve global security.

References

1. “Employees the biggest threat to network security” February 2005 Web. 20 July 2015
2. “SECLORE - What is IRM?” 2013 PPT slide 6. 7 July 2015
3. “IRM Oracle” October 2009 Web. 7 July 2015
4. “Configure your computer to use IRM” 2007 Web. 17 July 2015
5. “Restrict access documents Information Rights Management service”6 July 2015 Web. 7 July 2015
6. “Setting permissions on a mailbox” September 2007 Web. 18 July 2015
7. “How digital right management works?” 7 July 2015 Web. 7 July 2015
8. “Information Rights Management IRM not same as DRM” July 2014 Web. 7 July 2015
9. “iTunes and FairPlay” July 2015 Web. 13 August 2015
10. “Sony Betamax Case Summary” Sony Corp. of America v Universal City Studios 1984, pdf 20 July 2015

Copyright Statement