What is: Information Rights Management?

AUTHOR: GEOFF ANDERSON Business Productivity Advisor *Microsoft New Zealand, Wellington*

REVIEWED BY: JAY GARDEN Principal Consultant *High-Ground Information Security, Christchurch*

Information Rights Management helps organisations enforce, in the digital age, existing policies aimed at protecting confidential information and intellectual property.

Many organisations have policies relating to what employees are permitted to do, or not do, with the organisation's information. These policies may be included, for example, in staff handbooks or employment contracts.

It is surprising, however, how one person's view of what represents "confidential information" can differ from another's view, or how a staff member may assume that receiving a piece of information gives them implied authority to send it on to others.

Information Rights Management (IRM) helps organisations enforce information policies by allowing the author of electronic documents or emails to choose how recipients can use and share the information. This helps protect a company's intellectual property and helps prevent critical or damaging business information from being disclosed accidentally.

Empowering the document author

As explained above, IRM keeps the ownership and distribution rights of information where they belong – with the author. After all, if you are just asking someone to verify one statistic in one Excel Spreadsheet, why would they need to print the whole workbook out? Or, if a monthly sales pricing list is created, why would a particular person need it in six months?

Consider a scenario without IRM. You are developing a PowerPoint presentation for the board on a potential acquisition, and you need to ensure that it is accurate, so you email it to several people within your organisation. Once you hit Send, you have effectively lost control of that presentation. If the people you sent it to don't treat it with the confidentiality you expect, it is your bad luck – and it still has your name on it. In this case, of course, your reputation may be impugned if the information was seen to be disclosed before a planned market announcement.

IRM empowers you to protect yourself and your organisation from this scenario. Using IRM, you can click one button on the toolbar to protect both the email and any attachment before you hit Send. Now, your recipients can open it and make some edits, but they can't forward it. In fact, even if one of them copies the presentation to a disk and gives it to someone else, the document is protected so that the ultimate recipient will not be able to open it. With IRM, you know that only authorised people can open the presentation, so the information remains within your team – as intended.

The purpose of IRM is not to take capabilities away from authorised recipients of information. In fact, we find that communication frequently increases once people gain confidence that their thoughts will go only to intended recipients. The author's email address is always attached, and if people legitimately require additional rights they can always ask the author and the rights can be granted. But control remains with the author.

It is also possible to set up an organisational key so that the company can still gain access to documents which have expired, are required for legal purposes, or whose author has left the building (in the long-term sense!). Some organisations may also choose to further mitigate this risk with other policy positions – for example, by choosing to store controlled but unprotected master copies of key documents in a different location. This would give protection against any perceived current or future risk caused by issues or changes in the products or certification infrastructures that enable IRM at a technical level.

How it works

IRM allows you to set policies over who can open, copy, print, or forward information created in the professional editions of Microsoft Office Word 2003, Excel 2003, PowerPoint 2003 and Outlook 2003.

IRM relies on Microsoft Windows Rights Management Services (RMS) technology in Microsoft Windows Server 2003. Protection travels with the file so the information is protected, whether it is within your secure network or not. By mitigating accidental information sharing, IRM adds an important layer to the organisation's existing "perimeter-based" protection strategies. Because IRM transparently encrypts documents to protect them against unauthorised opening, the usual risks associated with the possibility of such encryption being compromised obviously need to be considered and balanced against the benefits of the additional protection that IRM offers under normal circumstances.

For the author, a document can be protected with one button from the toolbar of the application. More granular permissions can be set from the File menu, including selection of a predefined template (which the IT organisation has previously set up) or customised permissions. If an email is protected, any IRM-supported attachments in it are also automatically protected.

This level of simplicity makes it easy for existing users to leverage the IRM protection on relevant documents and emails. An organisation's IT administrator can also create templates that have specific permissions or groups of people (eg all employees) preset, so the functionality of IRM is set for specific organisational tasks, again making it easy for staff to adopt.

For the recipient(s), the process is even simpler. Upon opening a protected email or document, the application will check with the server that the user is authorised. Once this is confirmed, the document or email opens as normal. This process normally takes two to five seconds (this delay is a good incentive not to overuse IRM within an organisation!). Once the document or email has been opened once, by default it can then be read on- or offline by the same user with no delays on subsequent openings.

Balancing security and usability

Because IRM reflects existing policies and behaviours digitally, there is clearly some potential nuisance downside from over-protection. A good rule to promote with regard to information management generally is "a sensible level of security but a reasonable level of usability", and this applies to IRM use as well.

A sensible level of security. People using IRM should think about how protected they want a document, so that the level of protection matches the sensitivity of the document content. This is analogous to the various protection options available for paper-based information, ranging from "on the coffee table" to "in the CEO's safe".

A reasonable level of usability. The important flip-side of security is usability. IRM is designed to be simple to apply for authors and transparent to the recipient – as easy as learning other aspects within Microsoft Office such as Find and Replace, or the new Research pane. But that doesn't mean it should be used indiscriminately. A lot of information is valuable precisely because it can, does and should flow freely within and beyond an organisation – what we term "a reasonable level of usability". Moderation in all things leads to healthy information lifestyles.

A defence, not a panacea

IRM is designed to implement policy at a technology level. It will not stop wilful disclosure of confidential information to third parties. After all, an IRM-protected document can still be read out over the phone. What it does do is greatly reduce the chance of accidental disclosure, and increase the risks associated with leaking the information deliberately, as well as providing a trackable log of who has opened a document (and who has tried to open it).

It's also worth noting that IRM-protected files, like all encrypted files, cannot be scanned effectively by anti-virus software while they are stored in the file system. To mitigate this, we recommend anti-virus products that are integrated with Microsoft Office and scan documents as they are opened.

Who should use it?

IRM is primarily for use within an organisation, ie for internal information, protected by internal policy and used internally.

It is usually of highest value to those teams that deal with the most sensitive or business-critical information, such as CxO-level executives, finance and corporate services, marketing and human resources – although many companies find the idea of information being available to all employees, but protected from anyone else,

attractive. To find out what is the best use for your organisation, it is recommended that it is first piloted among key staff, based on a risk analysis of the information they typically deal with.

Microsoft's implementation of IRM has not been designed for home users at present, as they are not part of the authenticated domain infrastructure required.

Protecting non-Office information

IRM's potential is not limited to Microsoft Office. Once Rights Management Server (RMS) is licensed and installed on a server and client PC, developers can take advantage of it and write their own applications. Office 2003 is simply the first "out of the box" product to leverage the Windows Rights Management services. For example, an CRM application written in-house could potentially have rights management added for key functions.

A client-access licence for rights management services is required to access or create rights-protected content; organisations can license either users or client machines depending on which is more cost-effective. One licence covers the use of rights management services by all RMS-enabled applications used by that user or on that client machine, depending on the type of licence chosen. So a typical organisation wishing to use IRM will require a RMS infrastructure, then one RMS CAL and one copy of Microsoft Office 2003 Professional edition for each user who wishes to create protected content.

Deploying IRM

We recommend taking a measured and business-process driven approach to implementing IRM. Like most technologies, there is a potential downside if implementation is not well-planned. Well-implemented, IRM can be a significant step forward to sharing highly sensitive information with a wider audience, but if implemented casually it could also become an unnecessary IT headache.

User understanding and buy-in is a critical success factor. For example, by default, users will need to be connected to the network to open an IRM-protected document or mail the first time, and they will not be able to copy the file onto a home machine. (Of course, most organisations would not want files worthy of IRM protection on home machines anyway.) As long as users understand the constraints and the reasons for them, this will not present an issue, but as always lack of information will guarantee user frustration and an increase in helpdesk calls.

Deploying the technology is a typical two-step process of installing the Rights Management Server, then installing the rights-management client on PCs (Office 2003 will also need to be installed if it is not already). This is a similar process to installing and configuring, for example, Microsoft Exchange and Outlook. Although it is not technically demanding, many businesses prefer their technology partner to manage the project in order to leverage the experience of multiple implementations.

In addition, if an organisation wants to share rights with another external organisation, such as with their law or accountancy firm or a particular trusted supplier, it means setting it up to "trust" the other domain to allow for a two-way rights relationship. Again, a technology partner would typically implement this.

Do other vendors offer IRM?

There are other rights-management products in the marketplace, but to date Microsoft is the only vendor with a fully integrated, out-of-the-box offering. A key success factor is intuitive usability to drive adoption. Once installed, IRM technologies are easily made available in the Microsoft Office 2003 programs without significant additional training overhead.

IRM allows the author of a document or email to choose how recipients can use and share the information. This helps protect a company's intellectual property and helps prevent critical or damaging business information from being disclosed accidentally.

Information security is a top priority for Microsoft, which sees IRM technologies as playing an important role in helping users keep their information secure. It is expected that IRM will continue to evolve in the next wave of Office and Windows products, codenamed Longhorn.

Is IRM the same as DRM?

Digital Rights Management (DRM) is related but different from IRM. DRM is most typically used to protect the intellectual property of a vendor's digital product that is electronically sold into a wide market, such as music or film. If someone buys a music file online, for example, DRM built into the servers and players allows the licensor to control how the file is used. For example, the licensor may specify electronically that a music file can't be forwarded to others or copied, or that a video file may be watched for only a certain length of time.

DRM's focus on protection of intellectual property is based on the same technical principles as IRM, but IRM is specifically designed to address information protection needs within organisations, unlike DRM's "vendor-to-market" focus.

For more information see www.microsoft.com/rms.

The bottom line

- IRM helps organisations enforce, in the digital age, existing policies aimed at protecting confidential information and intellectual property.
- IRM keeps the ownership and distribution rights of information with the author, protecting them and the organisation from accidental leaks.
- IRM is primarily for intra-organisational use, ie internal information, protected by internal policy and used internally.
- Ensure a sensible level of security but a reasonable level of usability.
- It is usually of highest value to those that deal with the most sensitive or business critical information.

About the contributors:

GEOFF ANDERSON, the Business Productivity Advisor for Microsoft New Zealand, has a 14-year IT history. Over the past few years he has been providing specialist advice on how businesses can drive competitive advantage out of better use of their IT investments.
Contact: 04-474 7652, geoffan@microsoft.com.

JAY GARDEN is the Principal Consultant for High-Ground Information Security in Christchurch. He is a Certified Information System Security Professional and is SANS GIAC qualified.
Contact 03-365-0623, jay@high-ground.co.nz.