

Empower your business.*

Information rights management can
lock down confidential documents
and improve your security posture

Table of contents

The heart of the matter	3
--------------------------------	---

IRM provides powerful, persistent protection of sensitive company documents, no matter where they reside.

An in-depth discussion	5
-------------------------------	---

When confidential information falls into the wrong hands, the damage can be substantial—and often embarrassing.

Today there's more pressure for privacy, inside and out	6
Taking control: the power of persistent data protection	7
How IRM puts a lock on documents	8
Taking steps toward an interoperable IRM solution	9

What this means for your business	11
--	----

IRM can help a business thrive by providing the freedom to safely share information.

The heart of the matter

IRM provides powerful,
persistent protection
of sensitive company
documents, no matter
where they reside.

You are meeting with the marketing team, and the conversation is heating up. The marketing director is describing his frustrations with security measures the company has put in place to safeguard sensitive content.

The problem? He says the data protection policies hinder marketing's ability to send detailed project proposals to prospective vendors. Because of this, responses to RFPs are not as accurate as they could be. He argues that if marketing could provide precise (although confidential) details of product strategies, it would receive more accurate proposals from vendors. Projects could be wrapped up faster, more efficiently, and at lower costs.

You can feel his pain. After all, lost efficiency is everybody's business these days.

And then you deliver the good news: The security department can accommodate these requests by extending its recently deployed solution for information rights management (IRM) to the marketing division's sensitive documents.

This move not only frees marketing to do its job better, but also poises the company to grow its business and revenue. Employees—and the C-suite—begin to see security as a business enabler, not a cost center.

An IRM solution can provide comprehensive control over confidential content, boost employee productivity, and help reduce the likelihood of data breaches, whether the data resides inside or outside your network. IRM also enables you to “rewind,” or revoke access to, documents that have been distributed, giving you control of sensitive data throughout its life cycle.

Don't confuse IRM with identity management (IdM) or data loss prevention (DLP). IRM does not protect the network or application. Rather, it is a technology that safeguards data—Word and Excel documents, PowerPoint presentations, PDFs, email messages, and more—by applying fine-grained usage rights that describe exactly what users can do with the documents. More importantly, IRM provides a robust solution to persistently protect, control, and monitor sensitive content, regardless of the path it takes or application to which it is written.

IRM is an ideal complement to DLP and IdM solutions. Its anywhere-anytime data protection solves a huge issue for CISOs, compliance officers, and business executives. In the past, they had to worry only about information stored on servers and laptops. In today's world, email, USB thumb drives, laptops, and smart phones mean that data can—and does—go just about anywhere. Data leaks proliferate, whether accidental or intentional, introducing potentially costly and damaging risks to organizations' reputations.

IRM will help plug these data leaks so that sensitive content, regulated data, and intellectual property are protected no matter where they reside.

An in-depth discussion

When confidential information falls into the wrong hands, the damage can be substantial—and often embarrassing.

IRM is a technology whose time has come. Today, employees share information freely inside and outside the corporate walls, with results that are not always beneficial to the business.

Consider the case of one US mega retailer. Over the past few years, the retailer has experienced widely publicized incidents in which employees posted secret—and very sensitive—company information on the Internet. In 2005, a confidential memo about possible cuts in employee healthcare benefits hit the web like a virus, sparking a volley of complaints from union leaders. More recently, an internal PowerPoint presentation that detailed controversial opinions about a customer survey was published on a blog and made available for download—to anyone with an Internet connection. A well-designed IRM program would have prevented these damaging leaks.

Although this retailer fell victim to insiders, the potential for maliciousness extends to departing employees. A study by the Ponemon Institute and Symantec Corp. found that 59 percent of employees who left a job in 2008 admitted to stealing confidential company information, such as employee records and customer data. Most (53 percent) copied the data onto a CD or DVD, while others (42 percent) lifted data via a USB thumb drive. Many (38 percent) simply attached a file and sent it to their personal email accounts.

Often, unauthorized access occurs after accidental loss or theft of portable devices. The proliferation of portable electronic devices such as laptops, PDAs, BlackBerrys, and USB drives is a security challenge for most organizations today. In fact, theft or loss of a laptop computer or other accidental exposure accounts for more than 35 percent of identity theft-related breaches.¹

A recent report by Cisco found two other common practices that contribute to data loss. Almost half of respondents (44 percent) said they share work devices with others, including nonemployees, without supervision. In a result that will surprise few CISOs, 22 percent of employees said they carry corporate data on portable storage devices outside the office.² What happens when the employee leaves that thumb drive in a restaurant?

Not all leaks can be laid at the feet of employees. Corporate networks are very porous today, and ensuring that all devices are patched to lock out hackers is a truly Sisyphean task. IRM can reduce or eliminate the need to patch networks because rights management safeguards the data, which makes securing the channel or data store less critical. If the network is breached, IRM provides a significantly improved layer of defense because the data itself is locked down.

¹ Identity Theft Resource Center, *2008 Breach Report* (January 2009)

² Cisco Systems, *Global Security Study on Data Leakage*, November 2008

But when data breaches do occur, they can be very painful. In this year's PricewaterhouseCoopers (PwC) security survey, a significant percentage of respondents cited negative business impacts from security breaches including financial losses (39 percent), theft of intellectual property (30 percent), compromise to brands or corporate reputation (27 percent), and fraud (21 percent), among other damages.³

On top of those, failure to comply with industry regulations that demand data privacy can result in costly civil and financial penalties. In fact, the average loss per data breach in 2008 increased by 5.6 percent from 2007 to \$6.65 million, or \$202 per record, according to a Ponemon study.⁴

Clearly, there are significant costs associated with data breaches. So CISOs must ask themselves, "Are we doing enough to protect our sensitive data?"

For many organizations, the answer will be no.

And that is why IRM has become essential. It enables businesses to simplify the paradigm by protecting one of their most important assets: sensitive content. No matter where it is located.

Today there's more pressure for privacy, inside and out

Now more than ever, personally identifiable information (PII), confidential corporate information, and regulated data must be carefully guarded. Over the past several years, we have seen an increase in security breaches that exposed sensitive consumer data, such as Social Security and credit card numbers. In fact, identity theft has comprised approximately one-third of consumer complaints to the Federal Trade Commission for the past three years.⁵

To safeguard PII, businesses must adhere to an array of external compliance mandates that may be specific to a single industry or extend across many market segments. For instance, financial services companies must adhere to the Gramm-Leach-Bliley Act for protection of banking customer records, and any company that accepts payment by credit card must conform to Payment Card Industry security standards. On top of that, healthcare organizations must comply with the Health Insurance Portability and Accountability Act, and any publicly owned company must meet the requirements of the Sarbanes-Oxley Act (SOX) for financial accuracy and accountability.

Compliance is a significant catalyst for security, but it is only part of the picture. Today's organizations must also worry about how employees (and outsiders) use their sensitive content. As we have seen, data can be shared in myriad ways, and if it is not locked down, organizations could sustain loss of sensitive information such as intellectual property or business-critical product development plans.

³ PricewaterhouseCoopers, *Safeguarding the New Currency of Business* (October 2008)

⁴ Ponemon Institute LLC, *Ponemon Data Breach Costs* (2009)

⁵ Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data* (2008)

Internally, companies also face a plethora of daunting requirements that IRM can address. For instance, the sharing of intellectual property is required more and more to truly innovate. But companies must be able to prevent employees and contractors from taking this confidential data with them when they are terminated or their contracts end. IRM persistently protects data no matter where the data is located, how it got there, or who owns it.

Rights management can help ease these challenges while enabling the business. Employees will be more effective because they can freely share data with contractors and prospective vendors, and the C-suite will worry less about potential theft of trade secrets, intellectual property, and confidential management plans, knowing that should the need arise, the rights to the sensitive data can be revoked.

Taking control: the power of persistent data protection

IRM empowers the security department to reach into the core of an enterprise and drive policy-based control of data across every functional unit. The security staff can determine not only who has access to the files, but also what each individual is authorized to do with the information.

The security team also can generate reports on data usage for proof of compliance at any time and place in the data's life cycle, no matter whether it resides on the corporate network, in the wilds of the Internet, at a business partner's site, or on a former employee's home PC.

IRM is particularly adept at protecting data that has slipped out of an organization's control. If, for instance, the mega retailer discussed earlier had used IRM to lock down its documents, the confidential PowerPoint presentation could never have found its way to the web and into the headlines.

Another powerful feature of IRM is its ability to "rewind," or revoke, access rights to documents. If, for instance, an unauthorized user tries to open a protected document, an IRM agent will, in real time, first check with the company's IRM server. If the user is not authorized to view the document, the system will expire that file in real time, rendering it useless without access rights.

IRM is an indispensable tool for companies that outsource parts of their IT functions to outside service providers or share data with external business partners. Rights management can help make contractors and partners precisely follow the organization's security guidelines by applying rules that limit what users can do with documents. You can, for instance, prohibit third parties from copying or printing a document—even after the document has left your network—by simply adjusting user rights.

Finally, IRM can help enhance compliance with regulations such as SOX. Sarbanes-Oxley requires that certain types of documents be examined periodically to review who has accessed the data. This process is typically carried out manually, often via time-consuming interviews. IRM can automatically analyze who has accessed what data when, a capability that can dramatically reduce audit fatigue, trim costs, and improve accuracy.

How IRM puts a lock on documents

Under the hood, an IRM solution comprises a sophisticated system of policies that automates data protection. A key difference between IRM and other security strategies is that rights management attaches fine-grained rights to the data, rather than to the data store in which information resides or the channel or network it moves on.

The technology does so by applying various permissions to files to identify what users or computers interact with the files and how the data may be used. In addition to these usage policies, rights management technologies include software that enforces the policies and delivers content for consumption by allowed users.

Anything that is created within the organization can automatically include baseline protection policies. For instance, any file that contains the phrase company-confidential would be assigned appropriate rights management policies.

These usage policies can be applied in myriad ways to protect data. Consider the average Word document, for instance. The IRM administrator could assign a policy to the document that specifies it can be read (but not saved) only by authorized users. The administrator can further lock down the document by setting an expiration date; when the current version is outdated, rights to open the document will be revoked so that up-to-date versions are always used.

The administrator could prevent distribution by adjusting the policy so that when the attached document is emailed, it cannot be forwarded or saved after it is received. IRM could even restrict printing, copying, pasting, or screen capture, among many other actions. And if the authorized user becomes unauthorized (after termination or a change in roles, for instance), he would lose all access to the document.

Whatever the usage policies, the document's owner has the ability to analyze the use of the data and take action in the event of suspicious activity. For instance, if a Word document's policy requires it must be read by a specified date, the rights holder can determine whether the document has been opened and the reader forwarded, saved, or printed it. Usage rights can be revoked if the document is inappropriately handled.

Taking steps toward an interoperable IRM solution

It is tempting to approach IRM as a purely technical initiative that can be realized by simply adding software to the IT infrastructure. But that is a one-sided approach that will likely prove ineffectual. IRM also requires a thorough, thoughtful assessment of the organization's processes and the commitment of each person throughout the enterprise.

As with many technology initiatives, the people part of the equation can determine the success or failure of the solution. The reason is simple: The hard work of applying a rights management solution centers on thoroughly analyzing individual business needs and processes. This careful analysis is ultimately a human task. Once completed, it can pay huge dividends.

In the earliest stages of a risk-based approach, the organization must determine its data protection requirements. IT will work with business unit leaders to root out the location of sensitive data and determine how it is used and by whom. The first step will be to create a data-classification guide, then develop role models that map user communities to sensitive data.

In the second step, the security team will consult with business unit leaders to study objectives and data requirements against state, federal, and international regulations. At this point, they should also have completed a risk assessment and prioritize data based on its value to the company. Every piece of data has its own value, and the organization should assign a value or categorize data during the planning process. For instance, your team's weekly status report may not be that compelling to an outsider, but advance information on the company's quarterly financial report certainly would be.

Next, the business will develop processes and procedures for updating policies and roles so that the IRM solution can keep pace with the content and future use of data. Because IRM systems must integrate seamlessly with other enterprise security solutions, it is essential to create and fine-tune content monitoring rules so that they are interoperable with the existing security environment, including IdM and DLP.

Once these issues have been resolved and the architecture has been mapped out, the IT department will test configurations, business and operational processes, and content-monitoring performance.

Sound complicated? It certainly can be. But our experience shows that, with the right expertise, the technology can be put in place in a matter of weeks. Businesses typically begin rights management in the executive, legal, and human resources departments, then extend the solution to other business units over time. Our skills in implementation of IRM solutions can help expedite a deployment and deliver the value much faster.

What this means for your business

IRM can help a business thrive by providing the freedom to safely share information.

We believe organizations that proactively embrace the opportunities of information rights management will free themselves to thrive in today's turbulent business climate. We also know that, even though data loss prevention and identity management are essential solutions, only IRM can persistently protect, control, and report on the use of sensitive data, regardless of documents' location or ownership.

IRM also can empower employees to do their jobs more efficiently and without unnecessary limitations on company information. This allows them to confidently share sensitive content and intellectual property with partners and contractors, which can result in better and more effective business processes. As the company starts to win more business, security becomes a recognized high-value service rather than a drag on the bottom line.

Want to get started?

First understand that analysis of business needs and technology choices is a process best undertaken with the assistance of a trusted partner with strong strategic and technical vision. PricewaterhouseCoopers is a recognized leader in security consulting with solid experience in data classification, role definitions, and governance. We also can leverage our skills in the related fields of data loss protection and identity management to create an effective, high-value IRM solution.

How IRM completes your security landscape

Information rights management (IRM) cannot be an island in the corporate information technology ecosystem. Rather, it must integrate with other solutions across the enterprise, including identity management (IdM) and data loss prevention (DLP). But only IRM addresses data protection head-on.

IdM safeguards access to applications, not data. It delivers automated, company-wide management of user identities across all enterprise resources, both within and beyond the firewall.

But nothing in IdM prepares an organization to handle the challenge of terminating access to data once it is outside the application or contained within a document, spreadsheet, or presentation. So if an accountant in your

organization stores confidential data on a thumb drive and then loses it, IdM solutions will be of no help.

DLP, on the other hand, is designed to detect and prevent the unauthorized transmission of information from the computer systems within an organization to outsiders. Once a document is in the wild, DLP cannot prevent it from being accessed or manipulated.

IRM, therefore, is a logical extension to both IdM and DLP solutions because it specifically protects the data in a file, no matter what application hosts it, how it is transported, or where it ends up. It effectively closes the loop on an organization's security infrastructure by focusing squarely on sensitive content.

In a rights management implementation, knowledge of the privacy regulatory landscape is essential. After all, organizations must know precisely what data they are mandated to protect and at what level before they can identify and protect related content. Using our deep, up-to-the-minute knowledge of compliance, we can help you design a privacy impact assessment that spells out how rights management will protect regulated data.

PwC understands the optimal balance among strategy, design, and implementation services. Our mature perspective on security is part of a larger vision for a risk and security framework.

PricewaterhouseCoopers' strong global experience and diligent approach to account management make us a strong choice to help you watch over your organization's crown jewel: its sensitive content.

To have a deeper conversation on the topic mentioned, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

Brad Bauch
Principal, Houston
brad.bauch@us.pwc.com

Rik Boren
Partner, St. Louis
rik.boren@us.pwc.com

Kevin Campbell
Partner, Atlanta
kevin.campbell@us.pwc.com

Thomas J. Carver
Partner, Pittsburgh
thomas.j.carver@us.pwc.com

Michael Compton
Principal, Detroit
michael.d.compton@us.pwc.com

Shawn Connors
Principal, New York
shawn.joseph.connors@us.pwc.com

Scott Evoy
Principal, Boston
scott.evoy@us.pwc.com

Kurt Gilman
Principal, New York
kurt.gilman@us.pwc.com

Joe Greene
Principal, Minneapolis
joe.greene@us.pwc.com

John Hunt
Principal, Washington
john.d.hunt@us.pwc.com

Jerry Lewis
Principal, Dallas
jerry.w.lewis@us.pwc.com

Mark Lobel
Principal, New York
mark.a.lobel@us.pwc.com

Sloane Menkes
Principal, Washington
sloane.menkes@us.pwc.com

Joe Nocera
Principal, Chicago
joseph.nocera@us.pwc.com

Chris O'Hara
Principal, San Jose
christopher.ohara@us.pwc.com

Fred Rica
Principal, New York
frederick.j.rica@us.pwc.com

Andy Toner
Principal, New York
andrew.toner@us.pwc.com

This publication is printed on Finch Premium Blend Recycled. It is a Sustainable Forestry Initiative® (SFI) certified stock using 30% post-consumer waste (PCW) fiber and manufactured in a way that supports the long-term health and sustainability of our forests.



30% total recycled fiber