

# Securing and Tracking Business Information with Oracle Information Rights Management

*An Oracle White Paper  
Updated July 2007*

# Securing and Tracking Business Information with Oracle Information Rights Management

**Information rights management is a file-level protection technology that specifies who can access documents and e-mails and protects digital files from unauthorized printing, forwarding, or copying.**

## INTRODUCTION

Every day, organizations share millions of documents and files electronically. They are e-mailed outside the firewall, downloaded from Web sites, saved to flash drives, and burned to DVDs. The majority of this content is not sensitive or confidential, but a significant portion of it is. Board communications, intellectual property, trade secrets, compliance information, product plans, and pricing quotes are somewhat secure when stored within server folders, e-mail inboxes of intended recipients, and other corporate repositories. However, in this era of electronic information, content can easily move to desktops, laptops, and mobile wireless devices both inside and outside the corporate firewall—leaving files insecure and accessible by unauthorized users.

When sensitive or confidential documents can be untraceably opened, copied and forwarded anywhere, organizations face a formidable set of consequences. Data breaches and information leaks can lead to customer losses, decreased revenue, lawsuits, and damaged reputations.

How can companies mitigate these risks? Many organizations are turning to information rights management (IRM), a powerful, comprehensive solution that delivers protection of valuable digital information wherever it is stored and used. IRM helps organizations to

- Maintain control over sensitive information even after it has been shared
- Track copies of documents and e-mails forwarded to internal and external audiences
- Ensure valuable information is not shared with the wrong people
- Prevent unauthorized access to, extraction from, or editing of information
- Revoke access to information when business relationships change

## INFORMATION RIGHTS MANAGEMENT VERSUS DIGITAL RIGHTS MANAGEMENT

IRM evolved from digital rights management (DRM), but is a distinct and different solution.

Typically, DRM is a consumer-oriented application that restricts who can access, view, print, or download commercially valuable content. It is used to manage copyrighted information—for example, to restrict the number of times a song can be downloaded from the internet to various devices. The information that DRM manages is typically not confidential and loss of revenue is the main consequence of operating without it.

By contrast, IRM is a business application. It focuses on giving the right people access to organizational information and controlling who can view or edit that information. IRM secures sensitive and confidential content regardless of where it resides, and ensures only approved individuals can access it. The risks of operating without IRM extend beyond revenue loss to lawsuits and damaged reputations.

## TRENDS AFFECTING IRM ADOPTION

A number of trends and business practices have made content security an increasingly critical issue for organizations.

The two most obvious trends are the rising volume of business information and the increasing ease of sharing that business information. In a May 8, 2006, article, *InformationWeek* reported that the amount of data generated and maintained by many businesses doubles every 12 to 18 months. Never has it been easier to exchange this data with others. Commonplace technologies such as flash drives, e-mail, CD burners, and instant messaging make it nearly effortless to create, copy, and distribute information.

Other trends affecting information security are the related practices of offshoring and outsourcing. The expanded use of outsourcing and contract workers means intellectual property data is being shared with a growing number of individuals worldwide. Organizations sharing sensitive information with individuals outside the company and the country need ways to protect that information.

The expanding number of compliance mandates and increased focus on reducing business risks make information security a high priority within many companies. In many cases, regulations require that communications among partners, clients, and customers be secured and trackable.

Employee turnover within organizations is a fact of life. However, employees typically have access to proprietary business information that could be taken with them when they leave a company. To protect competitive advantage and prevent information leakage, companies need to be able to revoke and extend access rights based on employment status—even after an employee made multiple copies.

**“Information is one of our company’s greatest assets, and security of those assets should be a priority. All information in ‘strictest confidence at board level’ is encrypted, both current and historic. With Oracle Information Rights Management, the document is encrypted whether it is on a memory stick, a hard drive, or an e-mail inbox at home.”**

**—Mark Sheircliff,  
Group Head of Information Security,  
O2**

### Trends affecting IRM adoption include

- **Rising volumes of business information**
- **New devices that make it easier to share data**
- **Outsourcing to individuals in different companies and countries**
- **Regulatory and compliance mandates to secure information**
- **Employee turnover rates**

IRM solutions help organizations effectively tackle these content security challenges. In particular, Oracle Information Rights Management prevents unintended audiences from accessing highly sensitive and valuable information.

## **ORACLE INFORMATION RIGHTS MANAGEMENT**

Oracle Information Rights Management extends security, control, and tracking beyond an organization's own network to remote user desktops, laptops, mobile wireless devices, and more. It gives organizations control over who sees their sensitive information and when, where, and how it is used.

### **Key Benefits of Oracle Information Rights Management**

- **Ensure content security, enterprise-wide – no matter how many copies are made, or where the copies travel**
- **Securely communicate with executives and external board members**
- **Protect intellectual property, even if outsourcing or using contract resources**
- **Prevent unauthorized access to information about critical corporate transactions (such as mergers or acquisitions)**
- **Share, protect, and revoke third-party access to corporate information**

Oracle Information Rights Management uses technology that “seals” documents by using encryption to place an access-controlled perimeter around the document, e-mail or Web page. Sealing the information associates it with an IRM policy and gives it a digital signature to protect against tampering. This process guarantees sealed content is protected and can only be opened or accessed by authorized individuals. Each policy is stored and managed on customer-owned and -operated IRM servers and can be applied to thousands of files—allowing the solution to scale to an enterprise level.

Easy-to-install software agents enforce the IRM policies on end-user systems. These agents integrate seamlessly with existing business systems and operate within the document's or e-mail's native application. Oracle Information Rights Management supports the broadest range of document formats—including Microsoft Outlook and Lotus Notes, Microsoft Office, Adobe Acrobat, and image and video files—and the deepest range of application versions.

Unlike other encryption products, Oracle Information Rights Management continues working even after a document moves beyond the corporate firewall. It secures and tracks documents and e-mails everywhere they are stored and used. Just as it ensures that only authorized users have access to secured documents, it also audits all actual and attempted uses of documents and e-mails.

With Oracle Information Rights Management, organizations can change users' access rights at any time, even for document copies that might be burnt to CDs or DVDs. Automated rights caching and synchronization means users have a complete set of their rights when working offline, while still ensuring that rights can be revoked when necessary. This technology can also aid in version control by revoking access to obsolete drafts and ensuring that only the newest version of a document is accessed.

## **CASE STUDIES**

Oracle Information Rights Management can be used to support individual content security projects such as securing communications for a merger, sharing product plans with manufacturers, or sending pricing information to partners. However, Oracle Information Rights Management is also easy to run on an enterprisewide basis. In fact, many customers begin using Oracle Information Rights Management

for a single project, and then extend it to other areas of the enterprise to secure varied types of content.

### **Johnson Matthey**

**“[Oracle Information Rights Management] is a collaboration tool that enables us to address one of our greatest areas of business risk—information leakage. At the same time, we have achieved significant time savings in compiling and sharing this information safely and securely.”**

**—Paul Axworthy,  
Group IT Manager,  
Johnson Matthey**

FTSE 100 specialist chemicals company Johnson Matthey chose Oracle Information Rights Management to protect technical and commercial secrets. The initial IRM project was designed to reduce the risk of information leakage around critical information assets such as manufacturing methodologies, technical innovations, and commercial performance data. Using Oracle Information Rights Management, the company creates sealed Microsoft Word documents from sealed templates to control access to monthly technology reports and to streamline the report collation workflow. The implementation was so successful that Johnson Matthey has since expanded its use of Oracle Information Rights Management to protect sales data, marketing information, and board documents as part of a phased, enterprisewide rollout.

### **Beckman Coulter**

Medical device firm Beckman Coulter deployed Oracle Information Rights Management to protect a range of sensitive information used by approximately 500 field sales personnel. For years, the company had distributed a printed resource manual. The manual included sensitive information such as product details, pricing information, customer case studies, and competitive analysis.

To make this information easier to use and update, Beckman Coulter wanted to convert its printed manual to a set of electronic documents. The company wanted to ensure its confidential product and sales information was not used or distributed in unauthorized ways. In addition, the company needed a way to revoke access by individual when needed—for example, when a salesperson left the company. Finally, the company needed the ability to control versions so only the latest information was accessible.

To meet these requirements, Beckman Coulter replaced its printed manual with a number of sealed documents—each accessible only in accordance with the organization’s information security policy. Since this initial deployment, the company has adopted Oracle Information Rights Management as its corporate standard for protecting sensitive information.

### **Fenwick & West**

Silicon Valley law firm Fenwick & West needed a way to protect the sensitive business information it handles for its technology clients. The firm handles mergers and acquisitions worth billions of dollars and uses Oracle Information Rights Management to secure the highly confidential content created as part of these deals.

The firm’s clients also needed to comply with regulatory requirements that require protected information exchanges between companies and legal advisors. Oracle Information Rights Management allows Fenwick & West to protect the

“It’s important for us to protect valuable client data and transactions, especially in critical applications like M&A where clients are disclosing key information about business financials, executive information, compensation, revenue projections, sales projections, debts and liabilities, and so forth. Oracle Information Rights Management provides the perfect balance of control without being intrusive.”

—Matt Kesner,  
Chief Technology Officer,  
Fenwick & West

“[Oracle Information Rights Management] enables Vodafone to apply consistent and persistent information security controls across all areas of the business. We view this application as one of the key products to help drive the successful adoption of ISO 17799 within Vodafone.”

—Mike Newens,  
Property and Security Director,  
Vodafone UK

information and documents that are exchanged in nearly 700 Web-based “collaboration rooms.” These collaboration rooms are used to discuss issues that include taxes, litigation, intellectual property, initial public offerings, and mergers and acquisitions.

Fenwick & West is currently integrating Oracle Information Rights Management with Microsoft SharePoint to create secure portals that can handle an increasing proportion of transactions online.

## THE ORACLE INFORMATION RIGHTS MANAGEMENT ADVANTAGE

With Oracle Information Rights Management, organizations have an IRM solution that is

- **Secure and Auditable**—Oracle Information Rights Management is the only solution that secures and tracks all copies of documents and e-mails everywhere they are stored and used, even after they leave an organization. It helps organizations maintain complete control, for the lifetime of a document, over who can use their most sensitive information and when they can use it.
- **Transparent to Users**—Scalable, tamper-proof control that is fully integrated into an organization’s workflow means that securing documents doesn’t interfere with end-users’ daily tasks. Authorized users, from both inside and outside the organization, can easily create and use sealed documents. Employees can send secure e-mails within existing desktop applications. With Oracle Information Rights Management, understanding encryption keys or authentication mechanisms is not required.
- **Easy to Manage**—Although other IRM solutions require companies to create individual policies for each piece of content, Oracle Information Rights Management classifies documents into groups that share the same policy. These policies define the organizational roles that have rights to access specific groups of content. This classification structure allows companies to easily and quickly implement policy changes that can affect a large amount of content. For example, if an employee moves from one internal team to another, a company can simply change their access rights in one policy and it is applied to all documents within the corresponding group.
- **Easy to Adopt and Extend**—Companies can limit the cost of adoption by first implementing a solution that secures executive communications or external sharing of trade secrets. This requires minimal IT involvement while introducing the benefits of IRM to the enterprise. Later, companies can introduce additional components that extend the IRM policies to more enterprise business processes.

## **EXPAND ORACLE CONTENT MANAGEMENT WITH INFORMATION RIGHTS MANAGEMENT**

**Content management helps to decrease costs, automate processes, reduce resource bottlenecks, share content effectively, minimize the number of lost documents, and better manage risk.**

As the amount of content continues to grow within organizations, challenges with its creation, management, and distribution continue to grow as well. Organizations have turned to content management platforms to help them manage and secure unstructured content such as documents, email, paper, graphics, spreadsheets, presentations, video, and audio files. Content management helps to decrease costs, automate processes, reduce resource bottlenecks, share content effectively, minimize the number of lost documents, and better manage risk.

However, users often download managed files to their laptops, save them on flash drives, or email them as attachments to external audiences. Information rights management enables organizations to expand their enterprise content management vision to desktops and places beyond their corporate reach. By pairing both information rights management and content management technologies, organizations can properly manage and enforce content management and security both inside and outside the firewall.

**By pairing information rights management and content management technologies, organizations can properly manage and enforce content management and security both inside and outside the firewall.**

Oracle Information Rights Management is a part of Oracle's content management product portfolio. Over 6,000 customers use Oracle's content management solutions to help them proactively manage and secure content, increase productivity and reduce costs with an enterprise-wide content infrastructure. For additional information on Oracle's content management solutions, please visit [www.oracle.com/goto/contentmanagement](http://www.oracle.com/goto/contentmanagement).

## **CONCLUSION**

A growing number of trends are forcing businesses to increase the security of their confidential information. By specifying who can access documents and by protecting digital files from unauthorized forwarding or copying, an IRM solution helps businesses avert information leakage. In particular, Oracle Information Rights Management prevents unintended audiences from accessing highly sensitive and valuable information—regardless of where that information resides.



Securing and Tracking Business Information with  
Oracle Information Rights Management  
Updated July 2007

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
[oracle.com](http://oracle.com)

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Other names may be trademarks of their respective owners.