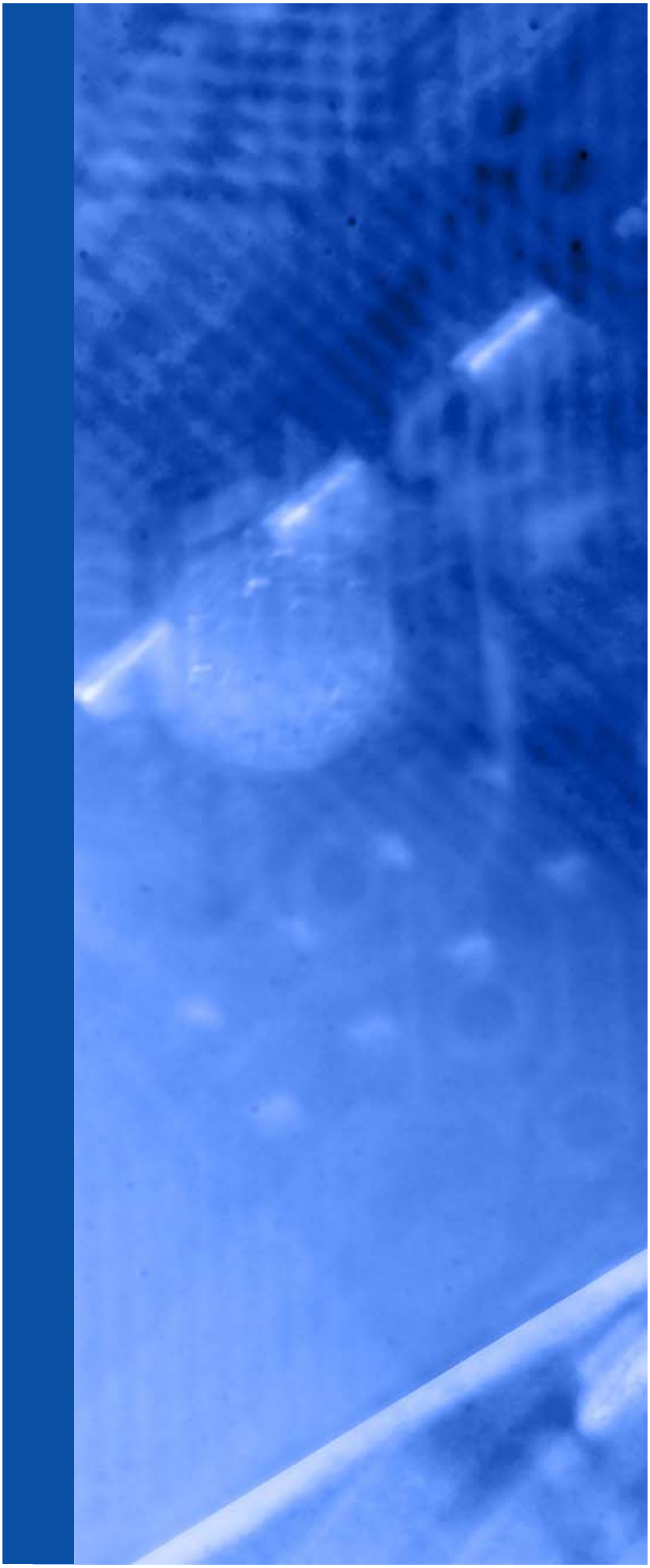

Research Report

Enterprise Rights Management

Business Imperatives and Implementation Readiness

August 2008

Bill Rosenblatt
David Guenette
Bill Trippe

THE GILBANE GROUP

Gilbane Group gratefully acknowledges the support of the sponsors of the research informing this report. This work would not have been possible without them. Please see the *Directory of ERM Solutions* **section of the report for descriptions of these ERM solution suppliers and their offers.**

Platinum

Fasoo.com

GigaTrust
Intelligent Rights Management™

Gold

EMC²
where information lives®

Microsoft®

Gilbane Group Inc.

763 Massachusetts Avenue
Cambridge, MA 02139 USA
Tel: 617.497.9443
Fax: 617.497.5256

info@gilbane.com
http://gilbane.com

Table of Contents

List of Figures

Preface

We have been following digital rights management (DRM) as well as content management technologies for many years. We have seen how some content management technologies that were originally applied to commercial media have migrated over the years to enterprise applications; the migration of DRM to the enterprise to become Enterprise Rights Management (ERM), also known as Information Rights Management (IRM) or Enterprise DRM, follows this pattern.

We have likewise been following the ERM market as it has come into its own over the past five years or so. But what may have seemed obvious to us, coming from the DRM field, has turned out to be far less than obvious to the legion of IT and security executives at corporations, government agencies, and other institutions who are tasked with controlling access to their enterprises' proprietary information.

The success of ERM in the marketplace is predicated upon both educating the marketplace about the technology and helping such executives understand how it complements their existing information security technologies. These are nontrivial, time-consuming processes. Only now are we finding significant but still early implementation of ERM. Therfore we felt that the time was right to check how far the market education processes have come.

Observing the actual marketplace, instead of projecting one's own ideas on to it, is one of the business analyst's biggest challenges, and accurately conforming one's timelines and expectations regarding the application of particular technology remains a difficult task. The key is to ask the right questions of the right people, listen to their answers, and acknowledge reality. Such a practice is simple in concept, less so in execution.

We believe that we've succeeded in coming up with the right questions and listening to the real answers. In part our success is due to the growth in the number of companies that are now considering implementing or have actually implemented ERM solutions, meaning that – for the first time—there is enough data out there to produce meaningful results.

We would like to thank our sponsors profusely for their support of this study, including their help in the often difficult task of securing customers for case studies. We would also like to thank all of our survey respondents, especially the ones who agreed to follow-up telephone interviews. Finally, we would like to thank Nora Barnes and her team at UMass-Dartmouth for their help in carrying out the survey.

Bill Rosenblatt, David Guenette, Bill Trippe, Mary Laplante

Introduction

Interest in Enterprise Rights Management (ERM) technology—also known as Enterprise DRM or Information Rights Management (IRM)—has been growing steadily since it became a technology category unto itself about five years ago. Now that many people consider ERM to be an adjunct to content management technology, the Gilbane Group has decided to start covering it in our research in the same way that we cover other technologies related to content management, such as collaboration, localization, and enterprise search. This study, our first in the ERM field, is the most comprehensive publicly available research on the ERM market ever undertaken.

After a brief recap of the history of ERM, we provide an outline of our ERM market study and some highlights of the survey results.

Background on ERM

Enterprise Rights Management is a direct offshoot of Digital Rights Management (DRM), the technology that was introduced in the late 1990s as a means of protecting media companies' copyrighted materials distributed over the Internet.

At heart, DRM entails encrypting files that contain content and only allowing those users or devices that have proper credentials to decrypt the files and access the content. DRM systems have these basic technology components[1]:

- **Content packagers**: software for encrypting files along with metadata.
- **License servers**: software for granting rights to users and/or devices to access encrypted files. In many cases, rights are represented in small encrypted digital files called licenses.
- **DRM controllers**: functionality on users' devices to request rights to encrypted files and to decrypt them for appropriate access when rights are granted. DRM controllers are often integrated with user applications such as word processors, media players, document viewers, etc., while others are integrated with users' PCs at the operating system level.

The first commercially available DRM technologies, from vendors like IBM and Electronic Publishing Resources (later Intertrust Technologies), were focused on copyrighted materials distributed to consumers. But some of the early DRM vendors understood that the technology could also apply to confidential information in corporations, government agencies, and so on; vendors like Authentica (now EMC) built DRM solutions that applied to both enterprise and commercial content scenarios.

There are some important technological differences between ERM and DRM for consumer content. For example, ERM solutions enable—or in some cases, require—

[1] Terminology for these components is not standardized; we take ours from B. Rosenblatt et al, *Digital Rights Management: Business and Technology* (M&T Books, 2001).

users to package (encrypt) their own documents at authoring time, from within applications such as Microsoft Office and Adobe Acrobat. DRM for consumer media entails content owners or distributors encrypting media files and sending them over the Internet to end-users. Accordingly, commercial media DRM usually works with "read-only" or "play-only" applications instead of content authoring tools.

ERM solutions also include sophisticated usage tracking and audit trail functionality, so that any misuse of confidential information can be traced. In contrast, consumer media DRM implementations are bound by laws and consumer interests related to privacy and so-called Fair Use of copyrighted material.

What we now call ERM began to drift apart from DRM for consumer content after the first Internet bubble burst. Many industry insiders point to 2003 as the year when ERM took on a life of its own, due primarily to two occurrences:

- DRM for consumer content became widespread through such applications as Apple's iTunes; it began to acquire negative connotations in the press because it was viewed as impinging on privacy and Fair Use. ERM vendors wanted to dissociate themselves from consumer media DRM, so they began pushing for separate terminology.
- A major software vendor marketed its own ERM solution for the first time in that year: Microsoft introduced Windows Rights Management Services (RMS). Microsoft had two different consumer media DRM technologies already out on the market (one for audio and video, the other for e-books); Windows RMS was built on almost completely separate technology. Microsoft introduced Windows RMS along with an ecosystem of solution partners, which included GigaTrust.

In addition, a few ERM vendors had large production deployments by that point—such as Fasoo's 50,000-seat installation at Samsung in Korea—which legitimized the technology.

ERM can be seen as complementary to content management. Content within a content management system (CMS) is protected, sometimes by sophisticated access control models, but when a user checks a file out of a CMS, it is no longer protected. ERM technology amounts to persistent protection for content. It can be integrated with CMSs so that content remains protected when it is checked out, and users can only invoke the rights that have been granted. Some ERM vendors began to integrate their products with various popular CMSs for customers.

2006 was the year when ERM became positioned more as an adjunct to content management. During that year, EMC acquired Authentica and began marketing it as an ancillary product to its Documentum enterprise CMS. During the same year, Documentum's competitor Stellent acquired another important early DRM vendor, SealedMedia; Stellent was in turn acquired by Oracle later that year. In 2007, Microsoft released an update to Windows RMS that integrated the product with its SharePoint Server CMS.

Yet ERM is not merely an appendage of the CMS market. Several standalone ERM vendors are still going strong, such as Fasoo. ERM is also complementary to other IT

security technologies, such as firewalls (perimeter security), two-factor authentication, and data loss prevention (DLP).

About the Study

We designed this ERM market study in order to get a sense of the progress that ERM has made in the market over the past few years since other studies were done, including a private multi-client study by JupiterResearch in 2004 and a public study by Sage Research in 2005 (no longer available). Due to the confidential nature of the technology, it is difficult to get reliable quantitative data about market penetration on which to base revenue projections. However, survey respondents' information about their own awareness of ERM, their ERM deployments or plans to deploy (or decisions to avoid the technology), and the applications for which they deploy it provide insight into market trends.

We also designed it to assist ERM vendors in positioning the technology to their customers. As with any major new enterprise software technology, there are questions about customer value propositions and sales targets that this study was designed to help answer. With our survey results in hand, ERM vendors should get a clearer picture of which industries are adopting ERM; who (by job function or title) has responsibility, resources, and budgets for implementation; what value propositions they may find most attractive; and their IT environments.

Here are some of the highlights of our survey results:

- **Awareness of ERM has increased** over the past few years, and vendors' efforts are paying off to evangelize the technology to professional services firms who can sell and manage customer deployments.
- Apart from IT and professional services industries (who stand to gain by implementing the technology for their own customers), the **financial services industry is showing the most uptake** of ERM.
- ERM is becoming popular for supporting **information usage regulations such as Sarbanes-Oxley** (accounting) **and HIPAA** (healthcare).
- Apart from regulatory compliance, we found that three types of **business processes** involving confidential information were the most prevalent for ERM implementations: **client/customer communications, financial processes, and medical patient care**.
- **IT managers and executives are the decision-makers on ERM**; they, more than others (chief executives, security managers, legal department, etc.) have authority, responsibility, resources, and budgets for ERM implementation at every level of the organization.
- A large proportion of respondents' organizations are implementing (or will implement) **ERM integrated with CMS** or some variant of content management technology, such as knowledge management or collaboration.
- **Infrastructural obstacles to ERM deployment are eroding**, including such obstacles as lack of identity management standards; organizations are now more ready to implement ERM.

The remainder of this study is organized in the following sections:

- Section I contains results of the online survey that we conducted, with the help of the University of Massachusetts at Dartmouth, along with anecdotal information gleaned from survey respondents who graciously agreed to follow-up phone interviews. This section presents conclusions and lessons for ERM vendors drawn from the data.
- Section II contains case studies of ERM deployments featuring our sponsors' ERM solutions, in industries that include government, telecommunications, transportation, healthcare, and more.
- Section III is a directory of ERM solutions on the market.
- Section IV presents ERM Vision Statements from the study sponsors.
- The final pages contain brief biographies of the analysts who designed and carried out this study.

I. Results of Survey

Methodology

The structured primary research for the study included a detailed survey of over 200 IT, security, and content management executives at companies culled from Gilbane Group's subscribership and input from sponsors. The survey was conducted online under management by the Center for Marketing Research at the University of Massachusetts, Dartmouth.

To augment the survey, the research team conducted in-depth interviews with:

- A selected number of survey respondents.
- Study sponsors for best practices information.
- Sponsor customers whose experiences are captured in the case studies published in this report. Their insights into real-world application of rights management technology also contributed to the analysis.

Respondent Profile

As Figure 1 shows, respondents covered a wide range of organization sizes, with a tilt towards smaller organizations.
Figure 2 shows a broad spectrum of industries represented but indicates a greater awareness of ERM among companies in the IT (software, Internet, etc.) industry and in professional services; the latter category includes management consultancies and law firms.

Respondents from professional services firms told us that they often need to follow the information access policies of their clients. Although relatively few of their clients actually use ERM, it turns out to be a convenient way for a professional services firm to be able to receive information from multiple clients while ensuring that it is treated according to each client's access policy.

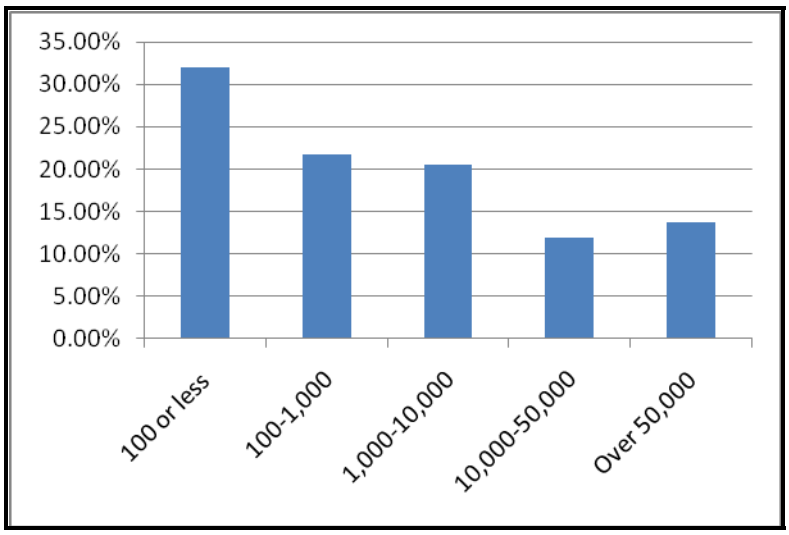

Figure 1: Sizes of respondents' organizations.

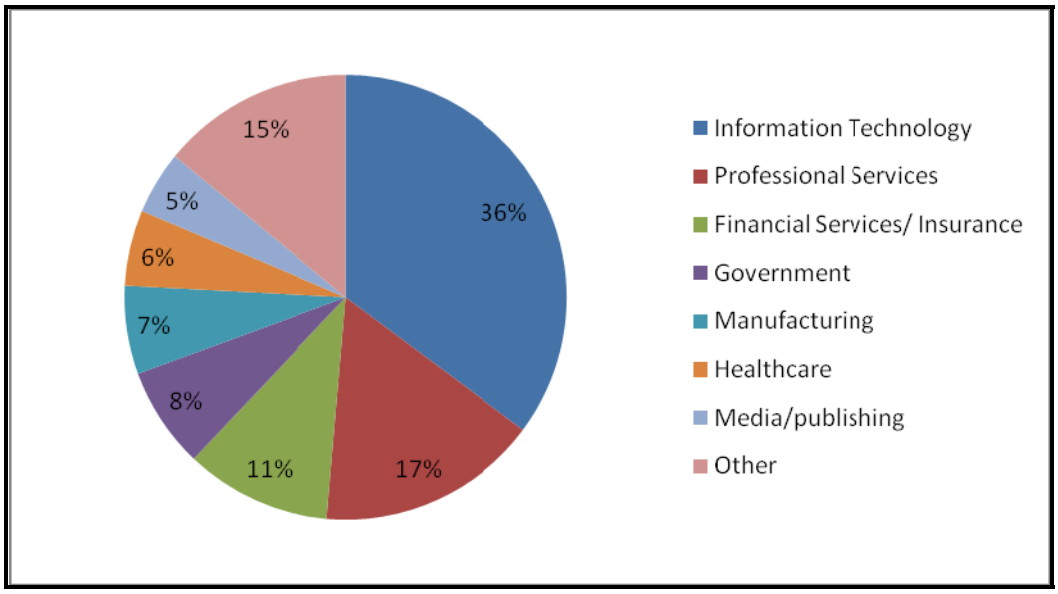

Figure 2: Respondents' industries.

Figure 3 shows that three-quarters of the survey respondents had at least some familiarity with ERM and similar terms, and only 8% have never heard the term.

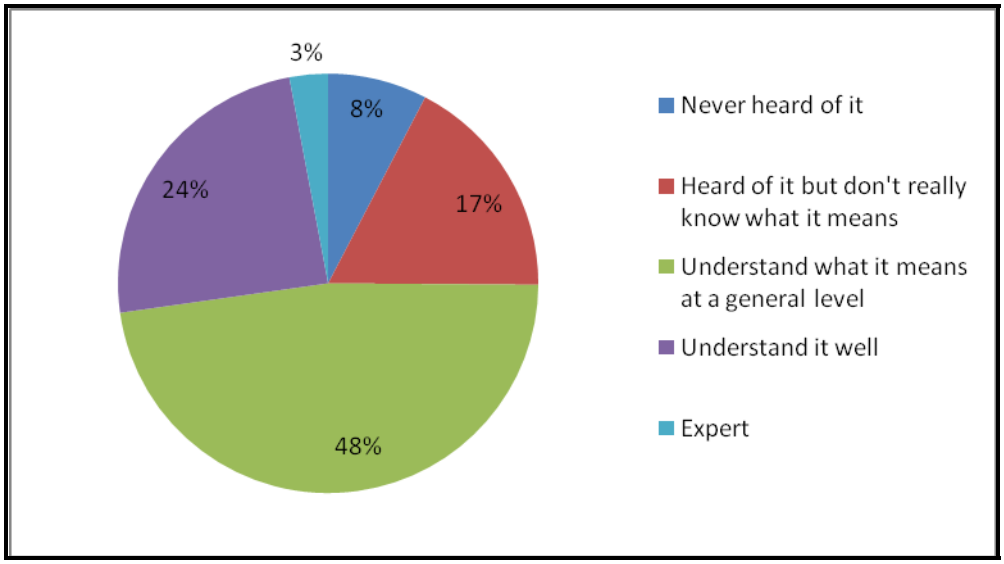

Figure 3: Respondents' familiarity with ERM.

Figure 4 shows ERM implementation status or plans of respondents. A quarter of respondents have implemented ERM, while about a third have plans to implement it at some point.

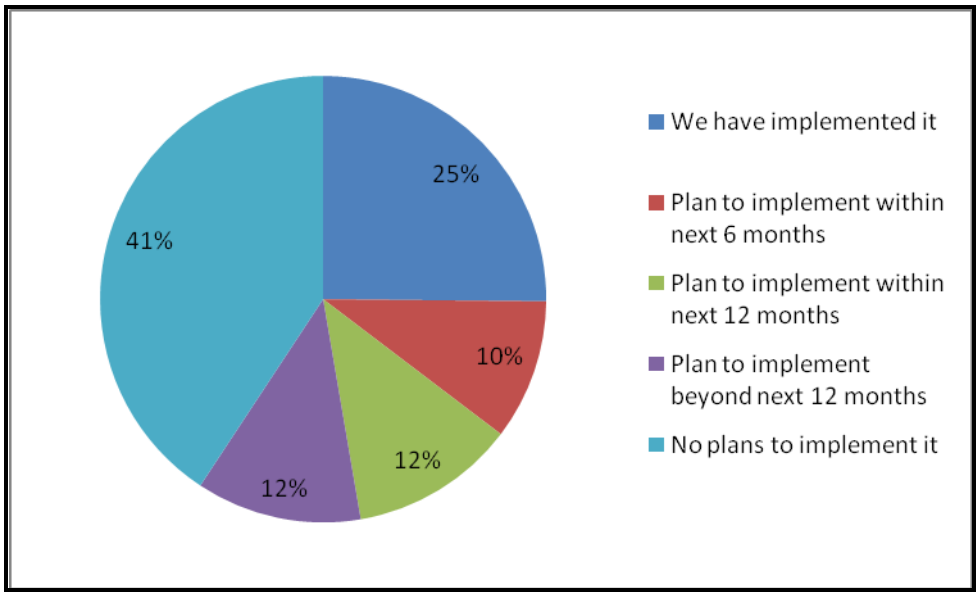

Figure 4: ERM implementation status.

One respondent from the insurance industry cited another obstacle to ERM deployment: the cost and effort in bringing documents under the control of an ERM system. The respondent's company has high volumes of legal and business documents, and there would be some effort in identifying documents that are current versus those that are expired.

For those respondents whose organizations have not implemented it yet, Figure 5 shows the reasons they gave. "Not a priority" was the top choice; other top reasons included complexity, cost, and usability. Only 12% said that there was insufficient business justification or executive sponsorship.

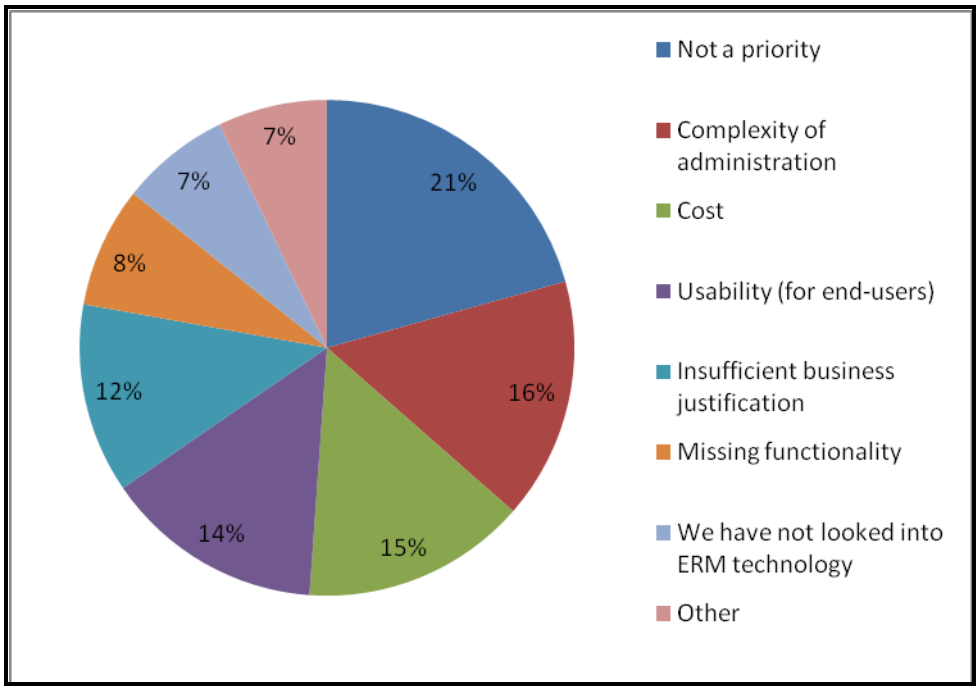

Figure 5: Reasons given for not implementing ERM.

ERM Deployments

Of those who indicated that they have implemented ERM in their organizations, half said that the scope of implementation was enterprise-wide, while 22% said that their implementation was at a business unit or division level. The rest of respondents' implementations were at the workgroup level or among specifically selected users. Figure 6 shows the sizes of these deployments, with 35% of them involving over 5000 users.

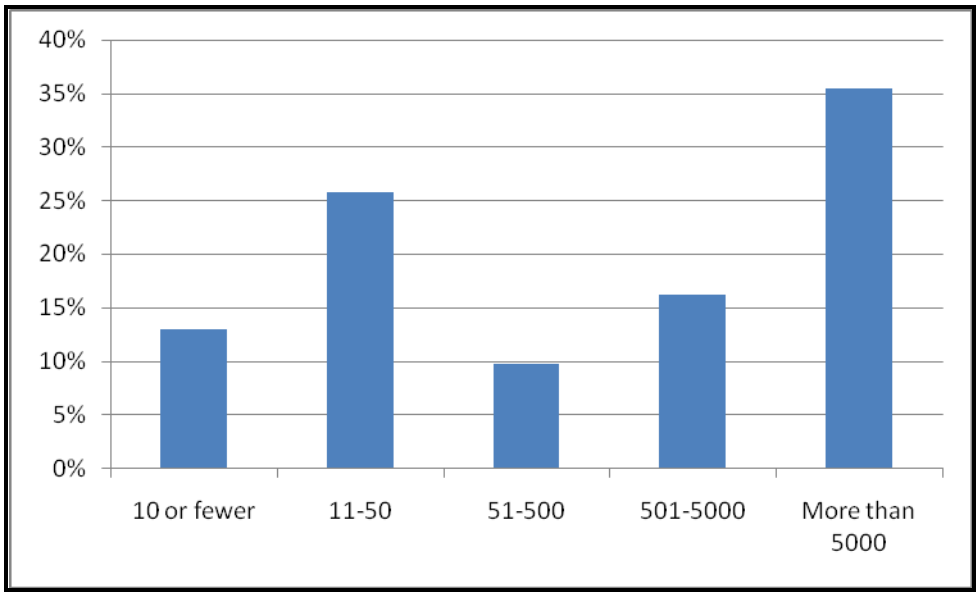

Figure 6: Sizes of ERM deployments.

Reasons for implementing ERM were spread fairly evenly. Although 25% claimed "Protect confidential information from leakage outside the organization" as their primary reason for implementing ERM, less than 20% chose each of the following non-exclusive alternatives:

- Restrict confidential information internally to only certain individuals
- Restrict confidential information internally to only certain job functions/titles
- Implement certain business processes digitally that otherwise would require hardcopy or face-to-face meetings to ensure security
- Enforce information usage policies that are currently written down, e.g., in a corporate policy manual
- Comply with industry information usage regulations or standards

Of the latter category, the Sarbanes-Oxley Act was the most commonly-cited regulation that respondents implemented ERM to support (24%), followed by the Health Insurance Portability and Accountability Act (18%) and ISO/IEC 27002 information security standard (13%). Other regulations cited included the Graham-Leach-Bliley Act

Title V, NASD Rule 1127, and the SB 1386 personal information privacy regulation in California.

When asked whether their organizations' business objectives are being or will be achieved through their ERM deployment, 52% said they are, 15% said they believe the objectives will be achieved, and 24% said it's too early to tell.

Figure 7 shows the applications and document formats that are used with respondents ERM deployments. PDF was the most prevalent (20%), with Microsoft Office formats (in the aggregate) very close behind, while email messages also proved popular (16%).

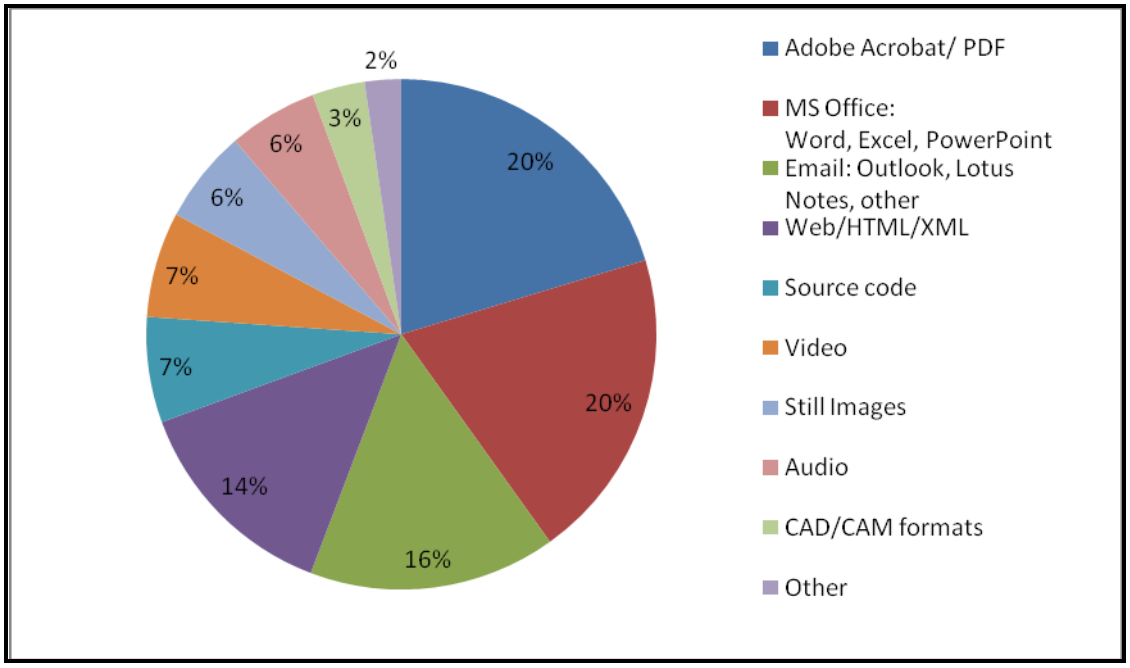

Figure 7: applications and file formats used in ERM implementations.

Figure 8 shows the types of server-based systems with which respondents' ERM implementations are integrated. Content and document management (taken together) are the most common category (24%). It could even be argued that knowledge management and groupware/collaboration also belong in the content management category, bringing the total to over half (55%).

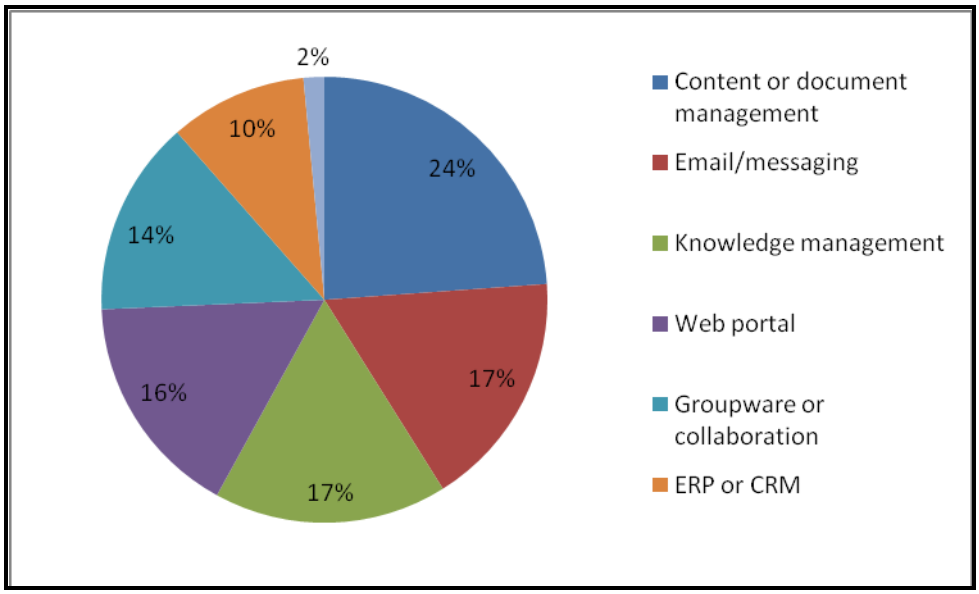

Figure 8: Applications integrated with ERM implementations.

Respondents' Technology Environments

We asked several questions designed to paint a picture of respondents' IT environments, to give an indication of the technology components and standards that ERM solutions should be able to integrate with.

Standardization on identity management is a prerequisite to ERM implementation, because ERM systems need to tie policies and rights on documents to identities (of users and/or devices) in a uniform way. We found that roughly equal numbers of respondents are using Microsoft Active Directory (31%), Windows logins (30%), and LDAP (25%) for identity management. Much smaller percentages of respondents are using X.509 certificates or other identity schemes. Fully 61% claim that their entire enterprise is on a single identity management standard. 17% asserted that each division, business unit, or workgroup used its own identity management scheme. 13% said that identity management is not used consistently in their organizations, and only 9% claim not to be using any identity management scheme.

For content management, the picture is quite different. 31% use a single, enterprise-wide content management system (CMS). 26% said that CMSs are used at the division or business unit level, while 18% said that they are used at the workgroup level. 26% said that content management is not used consistently in their organizations.

Figure 9 shows the different content and document management platforms in use. Microsoft SharePoint is by far the most popular, even more than custom-built systems. Documentum, at 10%, presumably represents larger organizations.

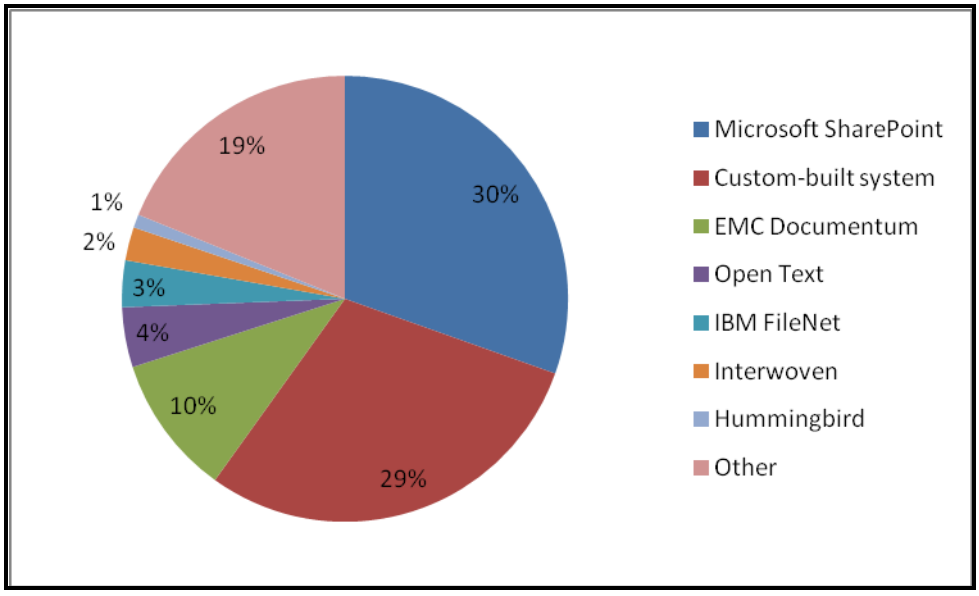

Figure 9: Respondents' content and document management platforms.

A wide variety of IT security technologies are in use at respondents' organizations, as shown in Figure 10. Firewalls (a.k.a. perimeter security) are the most prevalent (26%),

followed by virtual private networks (20%). 13% use single sign-on technology; the same amount use data monitoring or filtering.

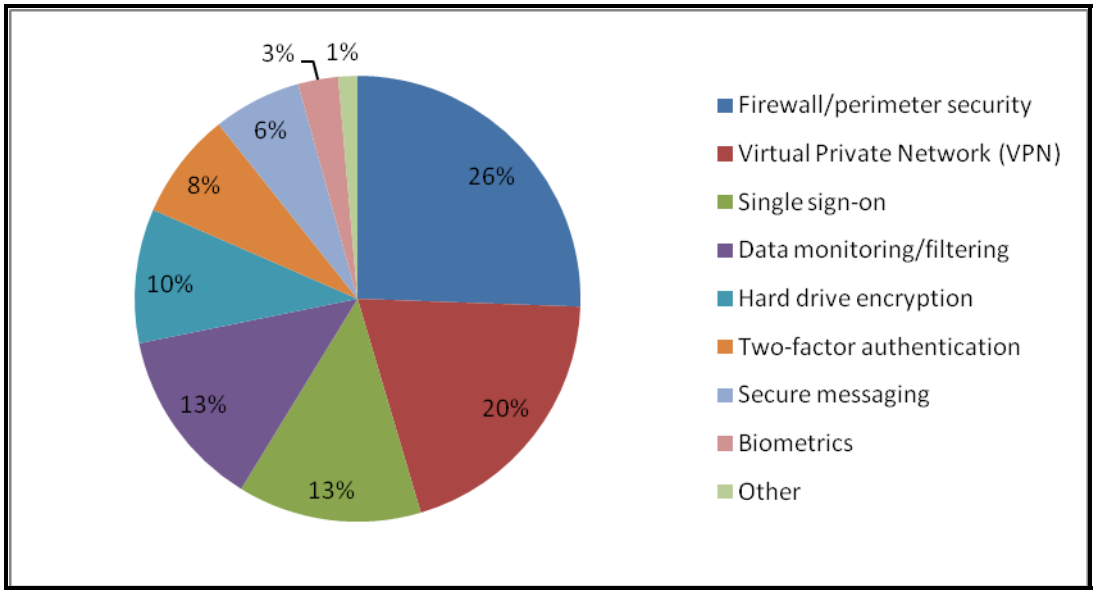

Figure 10: Security technologies used in respondents' environments.

Finally, the data on desktop client operating systems in Figure 11 shows non-trivial amounts of Linux and Mac OS among the Windows PCs. Windows operating systems in the aggregate amounted to 67%.

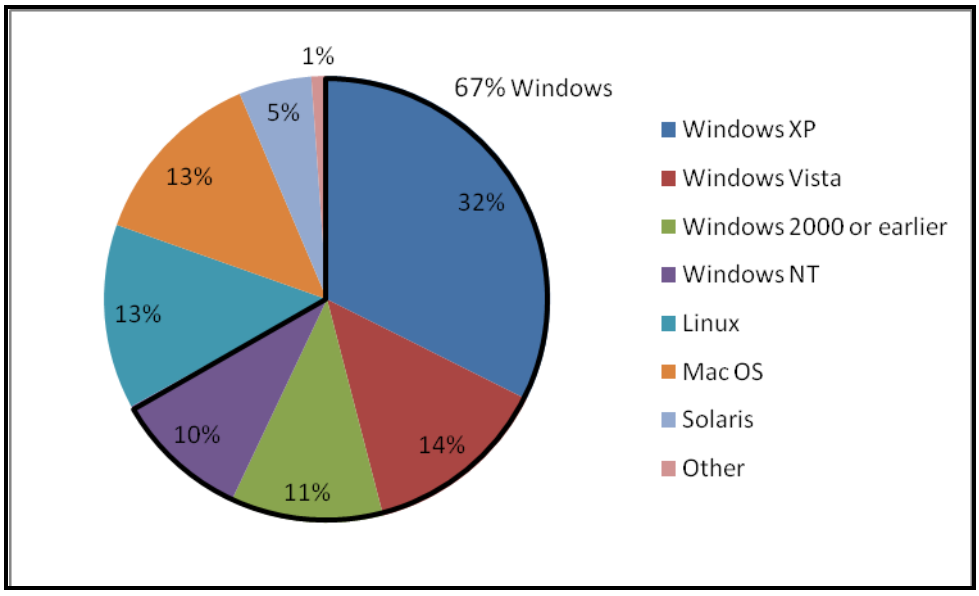

Figure 11: Client operating systems

Information Access Policies

We obtained information about organizations' information access policies, as an important component of ERM readiness. Organizations that have policies on information access that are clearly defined in detail, communicated to the organization, and consistently enforced are the best candidates for ERM implementation.

Over 80% of respondents said that their organizations had policies on information access. Of those, 64% claimed familiarity with them, and 17% of those said that their job responsibilities related to them. Only 5% claimed unfamiliarity with their organizations' information access policies. Figure 12 shows the degree to which information access policies are enforced.

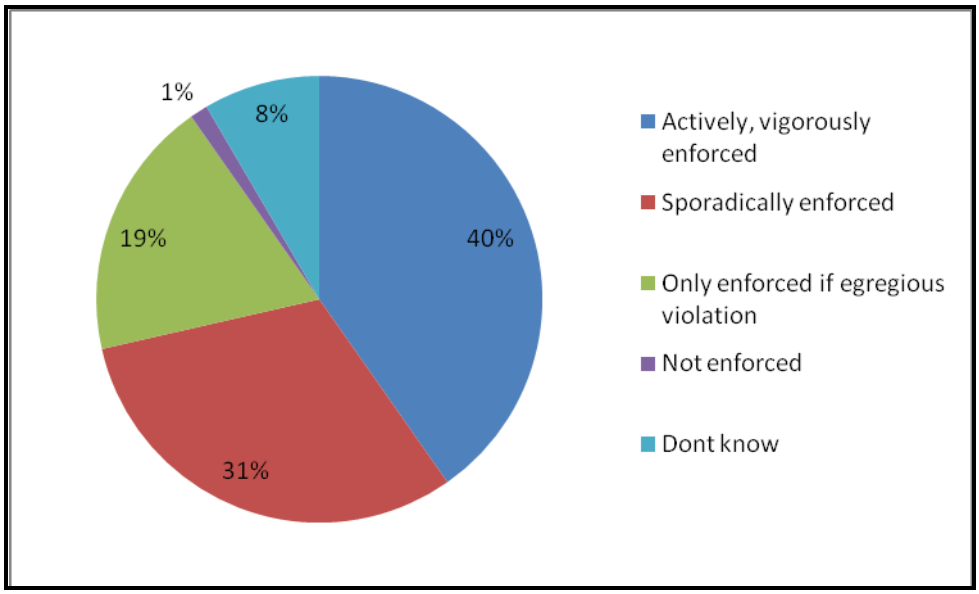

Figure 12: Levels of information access policy enforcement.

An important prerequisite to successful ERM deployment is that information access policies are given in sufficient detail to implement in an ERM solution. Almost three-quarters (72%) of respondents said that their policies are at least somewhat detailed, with more than a quarter (26%) being very detailed and thus possibly good candidates for ERM implementation.

Organizations with security technologies that are aligned specifically with information access policies are particularly good candidates for ERM. When asked about the alignment of technology with information access policies, over half (54%) said that the general goals of security technology and policies are similar. 23% said that they are well-aligned, that proactive security technology is implemented specifically to support stated information access policies. 15% said that their organizations' security technology has little to do with their information access policies.

ERM Decision Makers

We gathered information about the roles and titles of people at respondents' organizations who could be responsible for ERM implementation and have a budget for it. Our working thesis is that the ideal person to be responsible for ERM implementation is someone who oversees both security technology and information access policies; or, failing that, an organization where the executives in charge of each of those areas work closely together.

First we asked about responsibility for information access policies for the entire organization. Respondents supplied a wide range of job titles. We grouped these into categories, which are shown in Figure 13. The results indicate that the IT department (or equivalent, such as the CTO office or MIS department) is most commonly responsible for defining policies, followed by the CEO, President, or business head. Security or Information Security officers come in third.

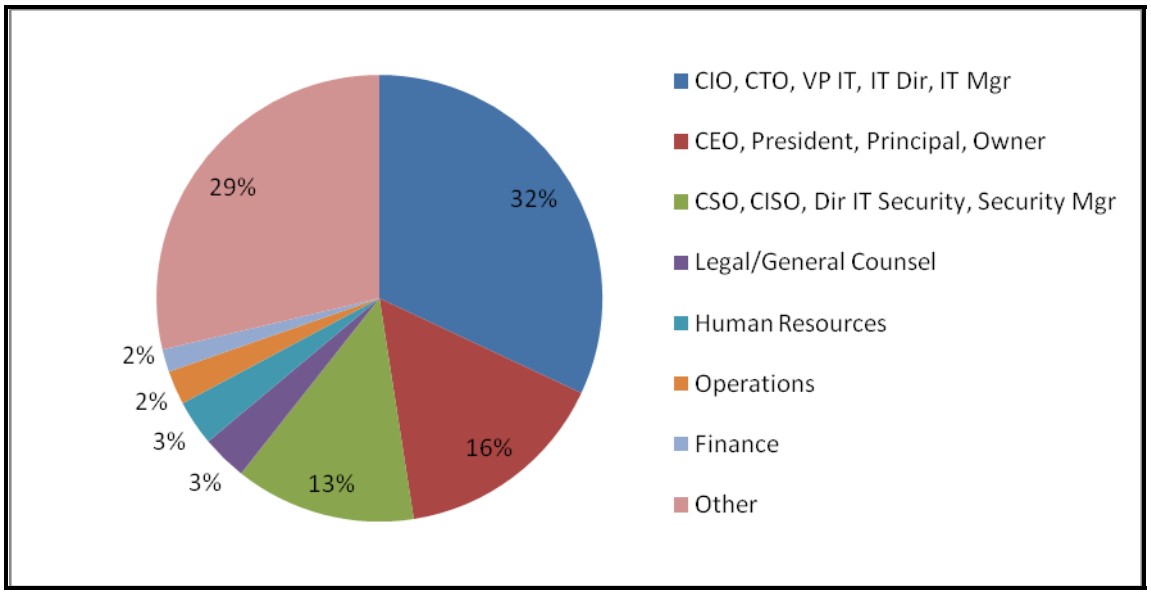

Figure 13: Job titles of those responsible for information access policies.

Of these, 45% of respondents said they had a budget for implementing technology to control information access, while 16% said they did not (the remaining 39% did not know).

Then we asked those who are responsible for IT security technology implementation and maintenance. These are shown in Figure 14. Here we see the IT or MIS department even more commonly responsible, followed by the security officer rather than the CEO or business head.

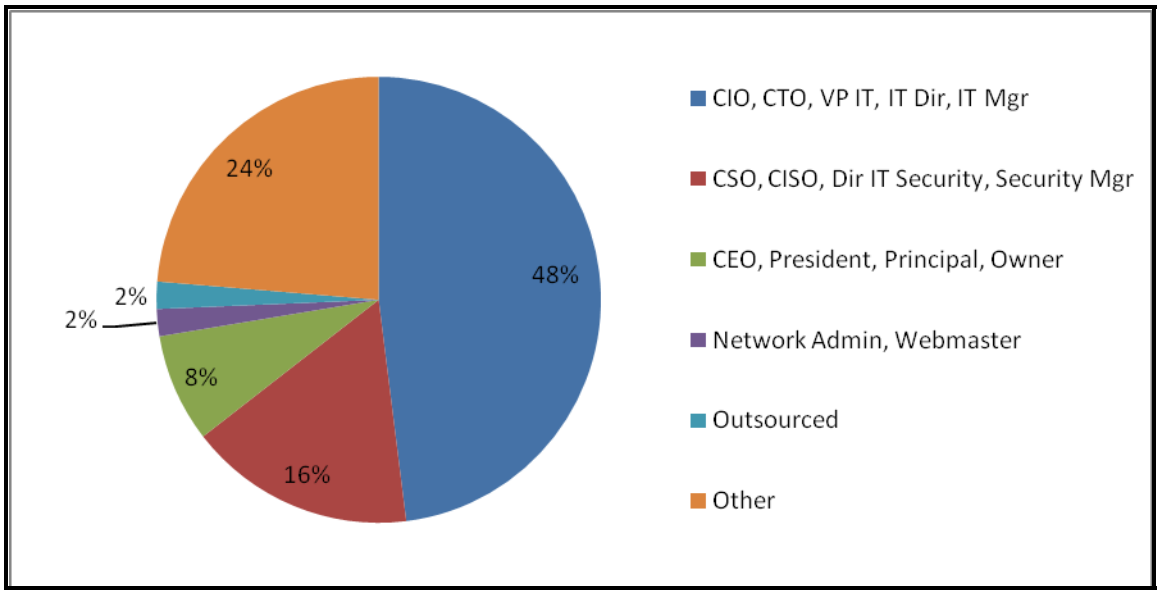

Figure 14: Job titles of those responsible for IT security technology.

Of these, respondents reported 53% as having a budget for implementing technology to control information access. 13% did not have a budget (the remaining 35% did not know). 57% were reported as having resources within his or her group to implement technology; 13% did not (30% did not know). We also asked if this person had resources in his or her group to implement the technology; the results were similar: 57% said they did, 13% said they did not, and 30% said they did not know.

We also asked if those in charge of information access policies and IT security technologies work together, even if they are not the same people or in the same department. Figure 15 shows these results: 63% of respondents said that they do work together at least "somewhat closely."

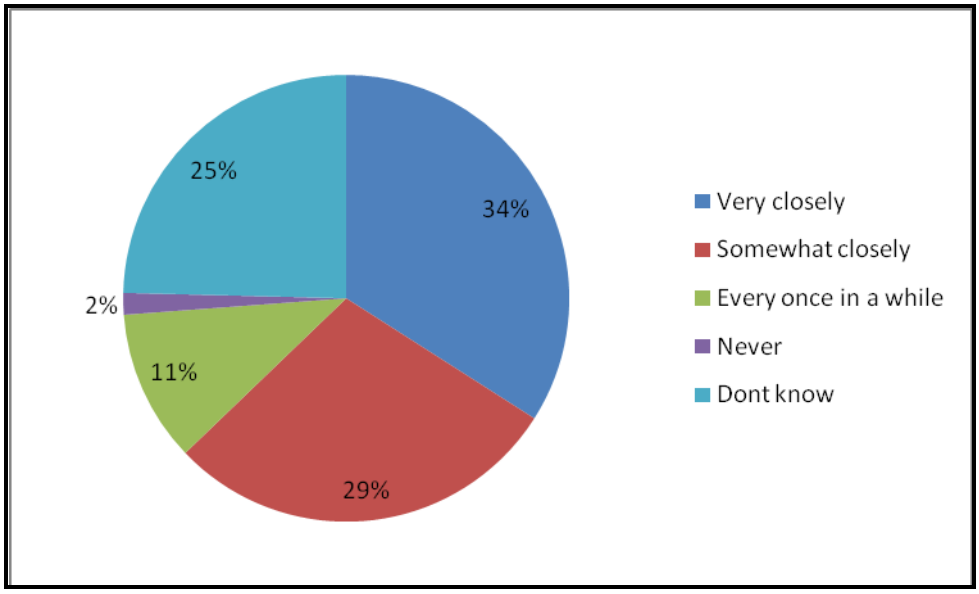

Figure 15: Indications of how closely information access policy and IT security executives work together.

We asked the same questions about executives at the workgroup, division, or business unit level (as opposed to the entire enterprise). 44% of respondents indicated that information access policies are defined for individual workgroups, divisions, or business units in their organizations, while 26% said they were not (31% didn't know).

Figure 16 shows which title or role is responsible for information access policies at the workgroup, division, or business unit level. Results were not unlike those for entire organizations in Figure 13, where 69% said that this person has a a budget for implementing technology to control information access (11% said he or she did not have a budget, while 20% did not know), and 67% said that he or she had resources to implement the technology (13% said he or she didn't, and 20% didn't know).

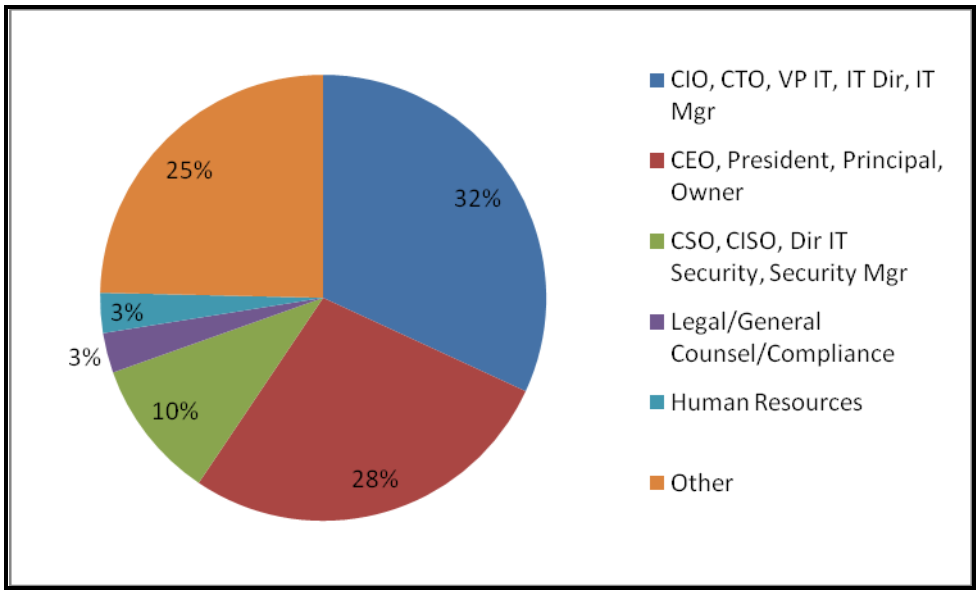

Figure 16: Job titles of those responsible for information access policies at workgroup, division, or business unit levels.

Finally, we asked about how well the risks of leakage of confidential information are understood in respondents' organization; a better understanding of such risks should lead to a sounder ROI case for investment in ERM. 38% said that leakage risks were understood "quantitatively and very well," while 42% said they were understood "conceptually but not quantitatively." (11% said they were not well understood, and 8% didn't know.)

We also asked which particular types of business processes had risks of leakage that were particularly well understood. This elicited a variety of responses, which we grouped into categories. The top three by a wide margin were:

1. Client and customer communications, CRM
2. Financial
3. Medical patient care

Other categories of business processes with well-understood leakage risks that were mentioned by multiple respondents, in descending order of mentions, were these:

- Intellectual property, including patent applications and copyrighted works
- Company confidential information
- Legal, litigation
- Product design
- HR, personnel
- Sales
- Supplier and partner communications
- Competitive intelligence
- Press releases, public relations, media
- Pricing

One respondent from the pharmaceutics industry told us of a need for ERM technology to secure information about drug licensing. Most pharma companies license drug R&D-related intellectual property in both directions: they license drugs in from other companies that they can manufacture and market themselves, and they license drugs that their internal R&D groups have discovered to other pharma companies that are more interested in or more capable of bringing them to market.

This process falls nominally under the heading of "intellectual property," but it also carries some flavor of the so-called virtual deal room in investment banking: a virtual space for reviewing confidential documents related to mergers and acquisitions that replaces a physical room to which concerned people must travel to look at sensitive documents.

Conclusions

Our survey shows that ERM is on a path of steady if not explosive growth, and that there are certainly opportunities for ERM technology providers to expand beyond generic solutions to those that target specific types of business processes.

The data show that **awareness of ERM has increased substantially over the past few years**. It is most instructive to compare our results with those of a study done in 2005 by Sage Research[2]; some of our survey questions were designed to echo those in the earlier study. In the Sage study:

- 26% of respondents had never heard of ERM or equivalent terms, while in our study the number was only 8%.
- 9% of respondents had already implemented some form of ERM, while in our study 25% had implemented it.
- In both studies, about one-third of respondents had some plans to implement ERM in the future.

A large percentage of respondents to our survey were from IT and professional services organizations. This indicates that such businesses see ERM not only as a benefit to their own organizations but also as a business opportunity. This in turn indicates that **more than just ERM software vendors are "spreading the news" about ERM**. Apart from IT and professional services, **financial services is the market with the most significant uptake of ERM**. This is not surprising, given that the financial services industry is typically an early adopter of related technologies such as document management.

There has been some question about whether ERM technologies apply to information usage regulations such as Sarbanes-Oxley (accounting), HIPAA (healthcare), and Graham-Leach-Bliley (consumer financial services). Our study shows that **ERM is indeed being used to support such regulations, with Sarbanes-Oxley and HIPAA** the most common.

Otherwise, while we can draw few conclusions about the general business reasons for ERM deployment, we can identify types of business processes that have well-understood leakage risks associated with them: **Client and customer communications, financial processes, and medical patient care are business processes where information leakage concerns are prevelant**, including intellectual property (patent applications, development of copyrighted works), development of company confidential information, legal/litigation processes, and product design.

---

[2] Unfortunately, this study is no longer available. For some highlights, see http://www.drmwatch.com/drmtech/print.php/3567756 or contact the lead analyst of this study. Of course, respondent qualification methodologies differed between this study and ours.

Our conclusion from this data is that **opportunities for ERM technology providers exist in the form of business processes rather than vertical markets**. ERM providers should tailor their solutions, product packaging, and messaging to those business processes, such as around secure client communications and collaborative development of intellectual property.

We asked several questions to help identify the most appropriate sales targets for ERM providers. It is clear that **IT managers are the right targets at every level of the organization**: they are most likely to have the authority to define information usage policies, as well as the authority, budgets, and resources to implement security technology. While security or information security executives tend to get involved in policy-setting, they are not the target customers.

Information gleaned from the survey about respondents' technology environments shows that **a large proportion of organizations will want to implement ERM in conjunction with some sort of server-based content technology**, including content management, document management, knowledge management, collaboration, etc. Microsoft components prove to be quite popular in respondents' infrastructures: SharePoint and Active Directory are the most prevalent content management and identity management platforms respectively.

Our data also shows that PDF remains popular for confidential information—even slightly more popular than Microsoft Office formats. Our conclusion: **ERM solutions should integrate with Microsoft environments, but should also support PDF**.

It is also worth noting that one of the excuses for not implementing ERM that we heard repeatedly in the past—lack of uniform identity management throughout the enterprise—is evaporating: 61% of respondents asserted that their entire organizations are on single identity management standards, and only 13% claim that identity management is not used consistently in their organizations. This means that **infrastructural obstacles to ERM deployment are going away**, an assertion further supported by the fact that about half of respondents who had actually implemented ERM say that their implementations are enterprise-wide.

II. ERM Case Studies

SI International: GigaTrust Helps Professional Services Company Facilitate Compliance, Protect Sensitive Data

> ***SI International wanted a better way to encrypt and protect confidential company information. Safeguarding documents with passwords didn't provide the right level of protection. When introduced to Microsoft Partner, GigaTrust, SI International found its solution. GigaTrust develops GigaTrust Enterprise software, which is built on Microsoft Windows Rights Management Services (RMS) for Windows Server 2003. GigaTrust software expands Windows RMS functionality beyond the corporate network and enables "on-the-fly" protection of content stored on Web sites built using Microsoft SharePoint products and technologies. Today, over 600 executives and support employees use Windows RMS and GigaTrust software to protect confidential information and to facilitate compliance. The company also obtained a solution that integrates with its existing infrastructure and applications.***

SI International is a premier provider of information technology and network solutions to Federal Government customers. Offering a wide range of services—supporting Federal IT Modernization, Defense Transformation, Homeland Defense, and Mission-Critical Outsourcing—the more than 4,000 employees at SI International use state-of-the-art technology to provide customers with "Rapid Response–Rapid Deployment" solutions.

Compliance and information protection: these two concerns are at the forefront of the minds of SI International executives. As a public company, SI International must comply with Sarbanes-Oxley Act (SOX) regulations and also safeguard material and non-public information prior to formal release—such as possible acquisitions, preliminary earning data, draft press releases, and similar sensitive items. SI International executives were concerned about preventing unauthorized access to this information. The company wanted a more intrinsic, practical way to protect sensitive information contained in documents and e-mail messages. In addition, the company wanted a way to post the information to internal Web sites built on Microsoft Office SharePoint Portal Server 2003 or Microsoft Windows SharePoint Services.

"We wanted to extend protection of confidential company information beyond the standard NTFS [New Technology File System] permissions on file servers and Web servers, and create a more enforceable way to apply company policies regarding how to retain the confidentiality of content," says Brian Beisel, Director of Enterprise Services at SI International. "In addition, we needed these rights-protection policies to be applicable to both internal employees working on the network, and business partners who don't have accounts within our network."

SI International was also interested in finding an information protection solution that automated the application of rights policies to data.

SI's Solution Search Parameters

As SI International began searching for something more than a perimeter-based security solution, the company saw a pre-release demonstration of Microsoft Windows Rights Management Services (RMS) for Microsoft Windows Server 2003. Windows RMS is information protection technology that works with RMS-enabled applications, such as Microsoft Office Word 2003 word processing, Microsoft Office Excel 2003 spreadsheet software, and Microsoft Office Outlook 2003 messaging and e-mail collaboration client. Windows RMS helps safeguard digital information from unauthorized use—both online and offline, inside and outside the firewall. Consequently, Windows RMS provides the first layer of data protection functionality that SI International requires.

Microsoft representatives introduced SI International to GigaTrust—a Microsoft Certified Partner and maker of GigaTrust software—and found the solution that fulfilled its additional information protection requirements. With GigaTrust for Enterprises, SI International can extend Windows RMS protection beyond the corporate network to its business partners, without requiring IT personnel to provision and manage external users. Then, by using GigaTrust for Web Servers, SI International can automatically protect content that is being published to its SharePoint Portal Server 2003 and Windows SharePoint Services Web sites.

Once the decision was made to implement Windows RMS and GigaTrust software, the deployment was fast. It took just one day to deploy the software to the SI International data center, and then another five days to roll out the solution to 20 pilot users. After a one-month pilot, the software solution was rolled out to over 600 employees working at over 100 locations and also to select business partners. SI International also customized the solution to establish several predefined security levels (confidential, sensitive, or full-access) that employees can apply to e-mail messages or documents that need some level of protection.

Windows RMS and the GigaTrust software are deployed on two servers running Windows Server 2003 Enterprise Edition. The Windows RMS and GigaTrust servers also interact with Microsoft SQL Server 2000 and integrate with Active Directory directory service, a central component of Windows Server 2003.

"SI International uses Active Directory to its full extent," says Nick Atalla Microsoft Strategic Partnership Manager for GigaTrust. "The tight integration of Windows RMS with Active Directory was an added bonus because the company was able to achieve an easy implementation without making significant changes to its infrastructure."

GigaTrust and Microsft RMS Benefits

With its Windows RMS and GigaTrust solution, SI International now has the technology in place that helps protect information, facilitates compliance, and integrates with the company's existing infrastructure and applications.

Seamlessly Protects Data at Desktop and Enterprise Level

SI International needed a technology solution that gives executives "peace of mind" that confidential data will be protected from both malicious and unintentional misuse. And today, it has that functionality with its Windows RMS and GigaTrust solution.

"The solution works. With GigaTrust and [Windows] RMS we can protect a range of document types (including PDFs) and content on SharePoint sites. There isn't an easier or more effective protection method available," says Beisel.

What's more, once users get use to the change in the process, it's an uncomplicated way to provide inherent protection on documents. "From a user's point of view, the solution is about as easy as it can be—the user just clicks an icon and decides the level of protection needed. The GigaTrust and Windows RMS software handles all the rest," says Steve Hunt, Vice President and Chief Information Officer for SI International.

Facilitates Compliance

One of the key reasons SI International implemented the Windows RMS and GigaTrust solution was to lock down access to non-public information so that it is accessible only to those executives who are authorized to view that information. This requirement helps ensure that the company is prohibiting pre-mature release of material, non-public information, and is complying fully with Security Exchange Commission requirements.

Hunt explains, "We wanted positive assurances that everyone was complying with the rules. For example, we need to make sure that sensitive financial information is not leaked to outsiders. With the Windows RMS and GigaTrust solution we're able to do just that."

Integrates with Existing Infrastructure and Applications

SI International extensively uses SharePoint—for its corporate intranet, storing proposals, collaborating on team sites, and leveraging SharePoint technologies to simplify coordination among geographically distributed management teams. With this breadth of usage, the company wanted an easier way to protect the information in the documents stored on SharePoint sites. With its Windows RMS and GigaTrust solution, SI International can apply unique permissions on specific sites within SharePoint and have the associated content protected "on the fly" as it is being stored and retrieved.

"For example, when we create a SharePoint site related to an acquisition or response to a government RFP [Request for Proposal], we apply GigaTrust to the entire site. This gives us added assurances that only authorized users will have access to the data and that they cannot send unprotected information out from that site," says Hunt. "In addition, the documents remain unencrypted while they are stored inside SharePoint so content can still be indexed and authorized users can use standard search capabilities; but as soon as a user tries to open or send a document, the rights management rules kick in."

In addition, the tight integration between Windows RMS and Active Directory provides an added bonus, as described by Hunt. “We are religious about changing or withdrawing rights and permissions from people when they move into different departments or leave the company. Because these permissions are all tied into Windows RMS, even if they take the document home with them and have it on a home computer, it remains fully encrypted until their access rights are reconfirmed by GigaTrust and Active Directory.”

This study appears courtesy of Microsoft and GigaTrust, and is accessible online at http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000021.

Veterans Affairs: GigaTrust Helps Win the Battle for Privacy

> ***The U.S. Department of Veterans Affairs had a close call recently, when confidential data about its millions of veterans was thought to have been released. By using Microsoft's Rights Management Server together with GigaTrust's Blackbery-enabled ERM, all is quiet on the privacy front, even while new services and functionality roll out across this enterprise.***

The United States Department of Veterans Affairs (VA) serves nearly 25 million American armed services veterans. With over 235,000 employees and a budget of over $70 billion, the VA is the second largest department in the U.S. federal government after the Department of Defense. Like its predecessor, the Veterans Administration, which was formed in 1930, The Department of Veterans Affairs was established as an independent agency, and was elevated to a cabinet level department by President Reagan in 1988.

The primary purpose of VA is to provide health benefits to veterans. The largest division of the VA is the Veterans Health Administration (VHA), which operates VA Medical Centers around the country; other divisions include the Veterans Benefits Administration (VBA) and National Cemetery Administration (NCA). Therefore, VA's information security obligations combine those of a military-related government agency with those of a medical care provider, making confidentiality of patient information a high priority. VA is divided into 23 smaller regional areas called Veterans Integrated Service Networks (VISNs), each of which has several thousand users.

The importance of patient information security at VA rose even higher in 2006, when two computers with confidential information on them were stolen: one with the social security numbers of all veterans in the VA system, the other with personal information about tens of thousands of veterans. The data was recovered, two men were charged with the theft, and tests found it unlikely that any confidential data was actually used.

Nevertheless, later that year, VA announced plans to beef up data security in various ways.

Security for Communication and Patient Privacy Protection

Higher-level managers needed to communicate securely. There is also a directive in place at VA to pull patient records at random to ensure that veterans are getting the proper care. There must be assurance that such records and documents are not used for any other purpose. Part of VA's multi-prong IT security approach was the adoption of Microsoft Windows Rights Management Services (RMS) and GigaTrust.

VA's Office of Information and Technology, run by General Robert Howard, took on this task. Architecture and development of the system fell to the Enterprise Infrastructure Engineering Group under Charlie DiSanno, including Jerry Taylor, Supervisor for Collaboration Services, and Dave Fish, technical lead for the project.

Fish did a lot of research into security software, and Microsoft had approached him to tell him about RMS as a way of achieving certain security goals. They set up a pilot installation of RMS.

VA chose RMS because it fit well with VA's existing infrastructure of Microsoft software, including not only Microsoft desktop applications , but also Microsoft Active Directory for identity management, Microsoft Exchange for email, and SharePoint for collaboration and content management.

The VA also chose GigaTrust because it offered crucial functionality on top of RMS, including client software for RIM BlackBerry portable devices and the ability to secure documents sent outside the firewall to external users. External users could be doctors communicating about patient cases with their professional colleagues at medical colleges or VA staff communicating with other agencies, such as the DoD. The ultimate vision for this huge department is to create a method for communicating with individual veterans, so that the VA can reach out to a veteran with the veteran's data and get it back again, updated all securely. The next best thing would be to send data to veterans securely, after which what the veteran does with his or her data is his or her own business.

Deployment: Microsoft RMS, then GigaTrust

The deployment of RMS to the more than 235,000 VA employees was planned in three phases:

1. Roll the RMS client software out to all desktops.
2. Procure and install new servers to run software, and roll out the GigaTrust BlackBerry components.
3. Set up the external provisioning functionality, which was to be the means of communicating documents securely to users outside the firewall.

Phase one took place over a four-month period and was completed successfully by the internal five-person team. It was done via a variety of ways:

- Microsoft Systems Management Server (SMS), which is a desktop configuration management tool for administrators that automates software licensing and distribution to corporate desktops.
- Active Directory Group Policy: with the Active Directory identity management server, which allows an administrator can define a policy that applies to all users in an organizational unit, and which includes the need for all users' desktops to have a certain software package installed. When an administrator defines such a policy in Active Directory, all users will have the software installed automatically overnight.

- Manual installations in those cases where the two automated techniques did not apply.

The RMS team went around to each VISN to sell them on the benefits of RMS. They created a training video, documentation, and an FAQ, which was posted on a SharePoint intranet portal. The RMS team developed a policy of producing new FAQ entries for questions and support issues that came up repeatedly.

For the deployment, each VISN provided one or two contact persons, who would set up the SMS packages and deploy it at the VISN level. RMS was initially deployed in VA's existing server environment, but the VA is currently in the process of porting it to new high-availability servers that were procured specifically to handle RMS.

The team is currently in the middle of Phase Two, which is being done with the help of Titus Labs for architecture and message classification (assigning security policies to email messages according to their content). They have tested and approved the GigaTrust software for the VA's current pool of some 7500 BlackBerry users.

Phase Three involves a number of more complex security challenges, including, for example, how external users can be authenticated, and how that process will be approved by VA's security specialists. With GigaTrust providing capabilities of authenticating external users regardless of whether their own organizations use Active Directory for identity management, the VA has the basis for a solution, but the protocols and procedures must satisfy VA security requirements. The RMS deployment team has not yet figured out how this will work.

Experiences: Fast Rollouts and More to Come

Dave Fish says that Microsoft "really did its homework" on the RMS client. "It went out there and for the most part just worked perfectly. It was shocking how successful it worked." With Active Directory Group Policy, the VA could deploy RMS to 15,000 users in about half an hour, and by the next morning, the RMS client would actually be deployed to that many users. For every such deployment, they might have had only three or four problems.

At this point, about 1-3% of the users are actually using RMS to encrypt and protect files. Users are asking the RMS team about when they should be using it, and the RMS team refers them to VA directives and policies about privacy and types of data that are considered sensitive. Such data can include personally identifiable information such as addresses, phone numbers, and social security numbers.

At this time, the most common usage of RMS is with email messages, which makes sense because people send information in email messages more than they create documents. Increasingly, however, users are asking about protecting documents that are posted on SharePoint portals and about protecting documents that need to be read only by a handful of specific users.

The RMS/GigaTrust team has experienced a bit of pushback. Some of this was due to the need to educate users about different approaches to data encryption. These users

needed to be assured that the architecture of RMS and GigaTrust conformed to VA security policies, which allow any scheme that is compliant with FIPS 140-2 (Federal Information Processing Standard on Security Requirements for Cryptographic Modules). Some users were under the impression that only the legacy PKI (Public Key Infrastructure) scheme was permissible for data encryption, which, although was not the case, required a surprising level of effort for education on this point.

The VA RMS team intends to quantify success of the project once all of the phases are complete and all the training is delivered.

Novation: Managing Access and Security of Sensitive Contract Documents with EMC Documentum Information Rights Management

> ***Novation is a leading contracting services company in the highly competitive health care marketplace. Novation's thousands of member organizations depend on Novation's clinical expertise and combined buying power to run efficiently. But some of this efficiency was being lost in a cumbersome process that kept member organizations from having timely and ready access to key contractual content. Novation identified IRM as the technology that could help them balance their need to closely guard contractual content with the need for authorized users from member organizations to access the content as needed. The Documentum IRM solution from EMC now allows Novation to share sensitive content with their members while also ensuring that only the right users can access, view, and print the content.***

With cost on the minds of consumers and professionals throughout the U.S. health care system, the procurement of supplies and services is more important than it has ever been. For major hospitals, hospital chains, and teaching hospitals, the combined buying power and expertise of Novation is a linchpin in helping these institutions operate more efficiently. Novation provides contracting services to more than 2,500 members and affiliates of VHA Inc., the University HealthSystem Consortium (UHC) and over 12,000 Provista customers. Novation's value proposition is both simple and compelling—to combine scale, agility, clinical knowledge, and product expertise in order to offer the most extensive range of advanced contracting services while delivering significant savings to its member companies. The scale is indeed impressive—VHA, UHC, and Provista members used Novation and alliance contracts to purchase $33.1 billion in supplies and services in 2007.

Based in Irving, Texas, Novation was created in 1998 through the combination of the separate supply programs of VHA and UHC. VHA, also based in Irving, is a nationwide network of more than 2,200 leading community-owned health care organizations and their physicians. The VHA network includes 27 percent of the nation's community hospitals. UHC, with headquarters in Oak Brook, IL, is an alliance of the clinical enterprises of the leading academic health centers. UHC's mission is to advance knowledge, foster collaboration, and promote change to help members compete in their respective markets. Provista, formerly known as HPPI, is one of the leading group purchasing organizations in the United States, serving over 12,000 hospitals, medical facilities, and colleges and universities.

Needless to say, with all of this purchasing come contracts, price lists, and other highly sensitive information that is confidential to Novation, its suppliers, and its member organizations. But it would be counterproductive to simply lock this content down. Member organizations are grappling with the need to deliver quality health care while

keeping costs down. Key individuals in these facilities need prompt access to the content to make purchasing and supply chain decisions; Novation needs to provide this access while also ensuring that the right individuals are accessing it and also controlling the details of access, viewing, and printing.

In addition to these core requirements of access and security, Novation faced a practical challenge of providing this content to thousands of member organizations—across a wide geographical swath and with the reality that these organizations have disparate systems, access controls, and platforms. Moreover, the contracts are viewed as highly sensitive, and Novation requires that the bare minimum number of physical copies of the contracts be available. Prior to automating this solution, Novation often found itself in having to travel to member organizations with a copy of the contract in hand, allow the right person to review the contract, and then return to Novation with the same copy of the contract in hand. This was clearly an impractical solution—not every organization could be visited in such a way, especially as the organization grew. Moreover, the member organizations were feeling the pressures of more competition and more scrutiny, and they were demanding more flexible access to the contracts so that they could ensure they were making the right buying decisions and were being as competitive and efficient as possible.

So out of this complex backdrop, Novation began to look at improving the processes of publishing and sharing the contractual content.

- In 2001, Novation implemented Documentum Web Publisher and Site Caching Services for publishing and maintaining web sites for member organizations.
- In 2003, Novation installed its first pilot of Documentum IRM Client for Adobe Acrobat for managing PDF copies of contract documents.

The current workflow has the signed contracts scanned, converted to secure PDFs, and then published to the web using Documentum Web Publisher. Authorized users at member organizations then log into the website and access the contracts. Depending on their level of access, they might be able to only open the documents or open and download a secure copy locally. Authorized users in the legal departments of VHA, UHC, Provista, and Novation can print the documents, as can certain selected member organizations.

These levels of access address the most common use cases Novation uncovered as it looked into the requirements of the IRM application. Within the member organizations, the most common users carry titles such Director of Materials Management, Director of Purchasing, or Pharmacy Manager, though in a smaller hospital or health care agency the user could be a CFO or CEO. They are most often asking a simple question such as, “What are the terms of the Novation contract?” and “Could we do better on our own or through another buying mechanism?”

Novation is now using the Documentum IRM solution to securely manage more than a thousand documents on its Intranet. There are currently approximately 3000 licensed users of the IRM technology, and in a given month several hundred of these users will access documents. Now more than four years into the implementation, Novation has

found that when users are active, they tend to be very active, reviewing many contractual documents in a short period of time.

With the contract management application in place, Novation is now looking at the IRM technology to help manage access to other sensitive documents and content. They have begun using the technology to manage internal planning documents (also PDF based for now), but are also eying an expansion of the technology to manage Microsoft Word documents, which are now primarily routed and "managed" in electronic mail.

With the expansion of document types, Novation has found a need to support new uses of the IRM technology and with it new IRM policies. To facilitate this, Novation has deployed a policy server that includes policy templates. For example, one policy template is used for internally distributed documents and has pre-configured rules for both user types and individual user (so this type of user can only view the document but these three individual users have the added permission to view and save the document locally). These rules can be based on single IP addresses, a range of IP addresses, or individual logins.

This same policy server plays a critical role in the workflow of a new document that is added to the system. The typical workflow now for a new contract is as follows:

- The contract workflow begins with the contract administration group (two people and a manager).
- The hardcopy of the contract is scanned and converted to PDF.
- The contract administrator opens the PDF and logs in as an author to the policy server.
- The contract administrator then secures the document to the contracting policy template.
- At this point, the secured PDF is imported into Documentum and pushed out to the website via a Documentum Web Publisher workflow and Documentum Site Caching Services.

Novation also has a "reverse workflow" for when documents expire, both for the IRM solution and for Documentum. Novation recognizes that the workflow could be further automated, and likely will when the volume of documents and the variety of IRM applications increases significantly.

Novation chose IRM technology from Documentum that includes the following components:

- EMC Documentum IRM Server
- EMC Documentum IRM Client for Adobe Acrobat

Novation has achieved several key benefits through the use of the Documentum products. These benefits include the ability to freely but safely share critical documents both within the organization and outside the firewalls, and a solid workflow and integration between its document capture process, IRM solution, and website publishing system.

The initial measures of success of Novation's IRM implementation are based on three criteria:

1. Whether critical contractual are properly secured.
2. Whether member organizations have ready access to these documents under appropriate controls.
3. Whether the document access improves customer satisfaction and supports the ability of the member organizations to be efficient and competitive.

By these criteria, Novation's IRM implementation has been successful. While Novation management initially monitored the IRM installation monthly and then quarterly, the system quickly reached a state where ongoing operations were routine. Novation cited recent examples where new and essential documents were placed online within a few hours for authorized users to then view and download the documents as necessary. And while Novation has never looked specifically at the cost savings of having a web site solution for document delivery instead of the burdensome processes they had before, they are confident that the system "quickly paid for itself."

Novation reported that the system implementation was very straightforward. The IRM solution was purchased in November of 2003 and implemented by the end of the year. Novation used EMC's professional services to install the software, configure it, integrate it with their LDAP environment, and set up the initial policies. This initial configuration effort took "one week" and Novation then tested the implementation and built the website interface. Novation reported that the EMC IRM solution is "not a big, complex system."

Given the large base of users and the guarantee of many heterogeneous client environments, one would expect some challenges in the deployment to the user base, but Novation reported only a few problems. The website was set up with instructions for users when they first logged on to access a secured document. They were provided with download instructions for going to the EMC website for the client application (a plugin to Acrobat). In a "handful" of cases, Novation ran into member organizations that strictly control users' ability to download client software. In these cases, Novation's IT group worked with the IT group of the member organization. In some cases, these IT groups wanted to control the installation of the plugins by pushing it out to user desktops themselves.

For Novation, the enterprise rights management application has solved a relatively straightforward but critical business requirement. Its large and widely disbursed customer base now has secure access to documents that help them perform efficiently in a highly competitive and ever-changing health market. Significantly, Novation has been able to do this at a reasonable capital cost without expending significant internal resources and also not taxing a customer base that was eager for a resolution to this critical business problem.

Korean Ministry of Information and Communications: Improving Policy Communication with Fasoo.com's ERM

> ***The Ministry of Information and Communications (MIC) is responsible for setting government policies affecting a huge range of telephone, data, multimedia, and IT issues for Korean corporations and citizens. The Ministry was the first major governmental enterprise to undertake a document management system aimed at improving the efficiency of policy formation among its key staff and outside partners, but it also discovered that it needed enterprise rights management (ERM) for the very system in place to develop these policies for other electronic media participants. Various products from Fasoo.com plug information leaks, while facilitating policy creation and workflow.***

The Ministry of Information and Communications (MIC) of the Republic of Korea is the government office in charge of industrial and public affairs concerning information technologies. MIC has recently been playing a pivotal role in Korean business as information technologies advance more rapidly than ever. One element of this work is the development of information technology policies; not surprisingly, sets of these policies involve information security matters. As it turns out, the work process on these and other policies exposes a potential security weakness: drafts, reviews, edits, and final policy publications are disseminated throughout the organization and out among key other key policy and industry participants, laying these documents open to unauthorized uses.

The Ministry of Information and Communications had its start as Korea's postal services, with the inception of the Directorate General of Posts in 1884. Among several significant other changes in this government department's history is the change to the Ministry of Communications (MOC) on November 11, 1984 to take care of postal services, telecommunications, life insurance, postal pension and government financial accounts. A decade later, it was expanded to the Ministry of Information and Communication (MIC) in order to unify the scattered functions of IT and strategically support the IT industry as an engine of the nation's economic growth. Today, MIC consists of more than three dozen divisions.

One often-stated goal of government innovation is to enhance efficiency of administration by improving the quality of its policy, and the Ministry of Information and Communication has energetically pursued this goal. MIC recognized the significance of establishing quality policies through systematic management and created the Government Policy Life Cycle System (GPLCS) in 2003. The GPLCS is a system that monitors the goal, implementation plan, and progress of government policies in real time. This system allows the instantaneous view of the policies in progress, shortening decision-making process and promoting information sharing. GPLCS is designed to clarify the goal of each policy by supporting the monitoring formation, implementation, and feedback of the policy in real-time, allowing high-

ranking officials—including minister and vice minister—to monitor the progress of each policy and set the direction for the ministry's overall policies and priorities.

Information technology and PC applications in place at MIC include Microsoft Office and various Microsoft operating systems, as well as Hangul Word Processor (HWP) a widely used Korean word processor, and a number of graphics and screen capture programs. MIC also employs various division- and ministry-wide server platforms, and some business process management applications, although MIC declines to be specific about them out of security concerns.

The GPLCS, while holding great potential, also presents significant risk. The Ministry of Information and Communication needed to protect confidential documents that are distributed in GPLCS (essentially an electronic document management system), while also requiring an overall tighter document protection system by protecting documents upon their creation. MIC decided to implement an ERM solution in order to mitigate risks of leakage as documents are passed along from one place to another both within GPLCS and outside of the system.

Security managers were primarily responsible for selecting ERM technology for MIC. The primary factors in choosing a solution were ease of use, integration with existing systems and applications, robustness and scalability, and the reputation of the vendor. Specific requirements included:

- Document protection for both GPLCS and for every PC in MIC headquarters
- Flexible document usage control for external (beyond MIC headquarters' networks) document deliveries
- Providing security and control of information from the MIC-related Web pages and printed documents

The Ministry has implemented ERM for the major information systems in its headquarters that support key policy establishment and management, as well as to all PCs in the network. Its security architecture includes identity management, perimeter security, and single sign-on capability.

Although MIC did not deploy ERM in order to enforce any specific information usage regulations, the implementation did have to be certified by the National Intelligence Service of Korea. A number of ERM solutions from Fasoo.com were selected by MIC over other vendors, largely because Fasoo.com has the largest number of public-sector customer references and was awarded a high level of security by NIS Security Certification.

The Ministry of Information and Communication chose technology from Fasoo.com that includes the following components:

- Fasoo Secure Document (FSD), for protecting and managing large volumes of documents stored in the knowledge management system and other systems
- Fasoo Secure Node (FSN), for protecting documents containing sensitive information that are created or copied on users' PCs

- Fasoo Secure Print (FSP), for preventing information leakage and tampering when delivering important documents outside the firewall.
- Fasoo Secure Web (FSW), for preventing information leakage and tampering when delivering important web documents outside the firewall.

The Ministry has achieved several key benefits through the use of the Fassoo.com products. These benefits include the ability to freely but safely share files both within the organization and outside the firewalls, and a smoothness of operation with GPLCS using flexible but seamless document usage control. The initial measures of success of MIC's ERM implementation based on two criteria:

1. Whether documents protected by the technology can be hacked.
2. How much the solution has increased employees' awareness of information security.

By these criteria, MIC's ERM implementation has been as successful as expected. In terms of risk management, MIC has achieved success by preventing leakage through persistent file protection (including encryption) and through audit trail data and tracing, if and when information leakage does occur.

Implementation troubles were typical of this type of ERM deployment: they consisted mostly of software conflicts—especially with Microsoft Office products, where the solution integration is based on application plug-ins. In such situations, the software vendor must act quickly to address software conflict issues, and MIC has had a smoother implementation than might have been, because of Fasoo.com's rapid technical support.

For the Ministry, enterprise rights management has enhanced employee awareness of information security to a remarkable degree. The initial phase of implementation has brought to light some user inefficiencies, most of which turned out to be due to the users' initial lack of familiarity with the ERM technology.

While not considered a perfect solution for eliminating information leakage, MIC believes that ERM technology like Fasoo.com's is the smartest and most practical way to minimize damage stemming from abuses of digital content. As yet, however, better incorporation of means to enhance privacy and police violations, as well as stronger ERM user convenience, remains for the future.

KT Freetel: Using Fasoo.com for Wide-Ranging ERM

> ***KT Freetel (KTF), the second-largest mobile telecommunications company in South Korea, provides a multitude of personal communications services in addition to voice, including multimedia messaging, entertainment applications, video content, email, mobile banking, home networking, portable Internet, and much more. KTF is exactly the sort of company everyone should be concerned about protecting content and privacy. The company has taken an active position in adopting enterprise rights management and has chosen a raft of DRM ONE solutions, from Fasoo, both as part of pressing business imperatives, but also in its exploration and appreciation of emerging crucial network-centric rights policies to control content not only within the enterprise itself, but, increasingly, among its partners and customers.***

KT Freetel (KTF) is the second-largest mobile telecommunications company in South Korea, majority owned by Korea Telecom, with annual revenues of KRW 6.5 Trillion ($6.9 Billion) and 12.9 million subscribers as of 2006. As Korea's No.2 mobile carrier, this enterprise controls about a third of the country's mobile market, which itself is the third largest in Asia. To generate greater data traffic, KTF builds on the extensive fixed-line networks of its parent, KT Corp., the country's dominant phone and broadband-service provider. While the market leader in South Korea is SK Telecom, KT F has emerged as a strong rival in offering new services such as live TV, video-on-demand, and music-on-the-go, all over its 3G networks. With three out of four Koreans carrying mobile phones, the rivalry between SK Telecom and KT Freetel has made Korea a test market for the industry.

What kinds of services are being tested in this real-world laboratory? KT Freetel Co. Ltd., through its subsidiaries, provides a multitude of personal communications services in addition to voice, including multimedia services such as multimedia messaging, color media downloads, multidata pack games, securities and entertainment applications, television services via the EV-DO network, video content, and email. This telecommunications company also offers services such as mobile banking, home networking, portable Internet, and telematics, as well as Nespot and Swing, which combine wireless local area network with mobile communications. The company describes its overall goal as creating a far-reaching partnership with customers through the concept of a “Personal Life Hub.”

In addition, KTF provides code division multiple access consulting, wireless Internet systems, network construction, investment, and network design/tuning services in India, Indonesia, Taiwan, China, Australia, Vietnam, and the United States. KT Freetel was established in 1996 and is headquartered in Seoul, Korea.

In such a competitive environment and as a core provider of so many services and products involving digital content, it is not at all surprising that KTF is security-minded. KTF implemented ERM in order to protect marketing and sales documents as

well as customer information. The ERM implementation helps KTF employees adhere to existing company regulations about information protection.

KTF's IT security infrastructure includes an identity management system, perimeter security, and single sign-on capability, and the organization has implemented enterprise rights management (ERM) in every business unit in a phased manner. The telecommunication organization started its ERM efforts within a key enterprise software application: the company's knowledge management system. Next to come was rights management applied to several internal information sharing systems, with company-wide implementation completed when ERM software on was installed on each and every PC on the corporate network.

KTF uses Microsoft Office on Windows XP and Vista operating systems, plus HWP (Hangul Word Processor), a widely used application in Korea, and various screen capture programs. In addition, KTF has in place servers for Outlook and Outlook Web Access (OWA) within Microsoft Exchange (MSE) that supplies the platform in which person-to-person (P2P) rights management happens. A local knowledge management system (KMS) called Acube, supplied by Samsung SDS is also in place, as well as a local business process management (BPM) system by Handysoft, which is tied to server-side DRM.

Of course, the more systems an enterprise launches to promote information sharing, the more potential for information leaks. The implementation and operation of KTF's ERM technology was driven by the IT and Security departments within the giant telecommunications company. KTF was looking for the most advanced DRM technology as well as proven deployment skills, and it chose Fasoo.com because this vendor had the largest number of reference customers in the world and thus had very wide experience in deploying the technology in a variety of enterprise environments.

The technology that KTF chose from Fasoo.com including these components:

- Fasoo Secure Document (FSD), for protecting and managing large volumes of documents stored in the knowledge management system and other systems
- Fasoo Secure Node (FSN), for protecting documents containing sensitive information that are created or copied on users' PCs
- Fasoo Secure Exchange (FSE), for preventing information leakage and tampering when delivering important documents outside the firewall.
- Fasoo Secure Web (FSW), for preventing information leakage and tampering when delivering important web documents outside the firewall.

KTF introduced its first ERM solution in 2002, when the technology was not widely familiar. At that time, KTF's employees were resistant to changes in the system environment, and faced some usage inconvenience concern about privacy issues. At the time, KTF implementers concluded that ERM vendors were less concerned about user-friendliness, while time-consuming custom development that was necessary whenever the company's users' operating systems were upgraded, or new application software added or PC hardware changed. KTF reports that these sorts of problems have been ameliorated through advancements in technology as well as Fasoo.com's active

technical support. Today, FSD's integration is required only with the company's authentication, user directory, packaging, and policy management applications, and Fasoo offers a standard API set for such integration, along with a growing catalog of integration samples with commercial products such as Documentum, Lotus Notes, MS Exchange, Humingbird, SAP, TeamCenter, and more.

Despite the difficulties incurred during the initial phases, there have been many benefits to KTF's ERM implementation. The risks of information leakage by insiders have been eliminated to a good extent, which means that IT staff can now focus on more productive matters than dealing with day-to-day security issues. As a telecommunications service provider, KTF uses several systems for electronic communication and collaboration and FSD, as well as other Fasoo-based ERM solutions, helps protect information distributed through or among these systems from illegal access or tampering. This in turn encourages KTF employees to successfully pursue communication and collaboration technologies without having to worry about the trivia of information security details, which leads to increased productivity.

FSD, which Fasoo considers to be the core infrastructure for ERM, allows KTF to create policies for content protection, manage and issue licenses conforming content to those policies, and track usage and behavior concerning the rights management content. The FSD's architecture is both Web- and server/client-based, and the original business applications operate transparently and without performance penalties along side FSD. After a file is DRM enabled, it is completely governed by the security policy that directs who can open a file for what purpose (e.g., view only, edit, print, and save), how many times, in how many PCs, and in which time frame. The policy can be changed any time immediately regardless of the location of the file, and he files are kept encrypted before and after use.

Generally speaking, the administration of any ERM system includes user management, policy management, key management, usage monitoring, and reporting. FSD exploits the functionality of existing application systems, and a single server of FSD can support multiple application systems and so minimize the burden of administration. Another feature of Fasoo Enterprise DRM Solution is that it conceals the key management completely, making explicit key creation, distribution, revocation, or backup unnecessary, placing the normal administration of FSD on policy management and usage reporting. By integrating the ERM policies tightly with the access control list (ACL) of existing systems, policy management can be further simplified. Even the deployment the client modules of Fasoo Enterprise DRM Solution offers very low oeverhead, because they are automatically installed and updated when they are connected to FSD.

Of course, many crucial files are created and saved on individual PCs, which can lead to improper disclosure or other security problem. KTF uses Fasoo's FSN, which protects PC-based files through automatic encryption. Document types handled "out of the box" include Microsoft Office, Notepad and Wordpad, and Acrobat Reader, while many CAD and image file types are also supported. Managers of user and user group information administer FSN's policies defining basic usage rights and terms, and the administrator can monitor and review usage logs.

While KTF's use of the various Fasoo DRM implementations contain persistent policy and protection functions for managed files, the company has a wide range of relationships with partners and suppliers outside the enterprise's network. KTF uses an email-based authentification system called FSE, which packages files sent by email with policies that include function enabling or restricting (such as print, edit, save, etc.), use number and expiration date restrictions, and file recall. The other means for information to geo beyond the enterprise is through the enterprises Web sites, and to solve the problem of protecting sensitive or licensed content presented in KTF's Web sites, the company uses FSW. The implementation of FSW is as straightforward as inserting a line of script into the relevant Web pages. Through the application of an ActiveX DRM client within the viewer's browser, print, copy, view source, save, save as, and other functions can be disabled for any selected or full Web page component.

While it is no surprise that control of information security is crucial for this large telecommunications company, whose very business is the creation and growth of networks among businesses and individuals, one of the unanticipated benefits of ERM at KTF is that it has dramatically raised awareness of information security throughout the company, particularly regarding customer information and company intellectual property. KTF's future plans for ERM include expanding it to apply to securely sharing information with its business partners and to use the technology to help the company conform to anticipated Korean government regulations on protection of customers' personal information.

Continental Airlines: Enterprise Rights Management in Practice, Using Microsoft Windows RMS

> ***In the last year or so, some of the business units within Continental Airlines began to see a need to protect and control certain kinds of content, but early solutions proved too limited to apply to the enterprise at large. When the Technical Unit in charge of enterprise-wide information technology architecture sought a better solution, they found one already largely in place, within the Microsoft Windows Servers and Office productivity applications. With modest efforts and very little additional cost, Continental Airlines is developing an enterprise rights management solution that can address the wide range of rights-oriented business requirements, through familiar platforms and interfaces that make adoption from the bottom up far more likely.***

We all know that business decisions are supposed to be handled logically, especially Information Technology (IT) choices. That's one of the main reasons for the existence of Continental Airlines' Technology Unit, at the giant airline's headquarters, in Houston, Texas. Jason Foster, System Architect for Servers and Senior Manager of Technology at Continental Airlines, knows this better than most.

And then there's the way business decisions often get made in the real world, which many times have little to do with centralized rational planning, but everything to do with addressing a sudden but pressing problem. As is often the case, the IT business unit gets asked for help after key decisions have been made. At the start of 2007, for example, Continental Airlines' Financial Business Unit realized that certain documents needed to have rights management applied to them, and specifically, for documents that get distributed to often widely-dispersed members of the Board of Directors and high-stakes executives who need to know essential proprietary information and sensitive financial numbers, such as earnings and revenue data. The Financial Unit looked to Adobe PDF and the Technology Unit was brought in, fait accompli, to implement a PDF-centric solution.

Foster, as server architect for the Technology Unit, was on the front line when the Financial Unit went to Continental Airline's Enterprise Project Office with the new project for rights management of financial documents. "All projects for the enterprise go through the engineering team for review and approval and we didn't have a rights management answer in place at that time. The Financial Unit had already looked at Adobe, and so we took the first stab with the Adobe Policy Server (APS)," Foster remarks.

One immediate limitation was that it was a standalone implementation of rights management that only handled the PDF document platform. According to Foster, another problem that soon became apparent was that it was pretty expensive to take into the rest of Continental Airlines. The Technology Unit took a deeper look at the Financial Unit's business requirement for protecting and tracking documents, but at

the same time looked to the other business units, to learn if there was any value to having an ERM (enterprise rights management) system.

The Starting Point: Existing Infrastructure

Continental Airlines already had widespread Microsoft solutions, including Microsoft Exchange and SharePoint servers, and enterprise implementation of Microsoft Office 2003 and (in some units) Microsoft Office 2007. "Continental has an enterprise agreement with Microsoft for our desktops, already has the Office 2007 and the entire suite license, and in that suite there was rights management as well," says Foster. "When we looked at what we have, to be diligent with corporate assets and software—in this case the licensing of Office is one of those assets—we took the original requirement of the Financial Unit to the HR and Legal Units and found that they too were very interested in a rights management solution." With Microsoft, given Continental Airlines' existing IT infrastructure, Foster could argue for using Microsoft's Windows Rights Management Services (RMS) on a favorable cost basis, too, since the corporation had already paid for the technology.

Overall cost includes implementation, and that sort of cost was on Foster's mind as the first quarter of 2007 passed and the difficulties with implementing the previous solution became clear. Foster noted that the Technical Unit at Continental is "more familiar with the Microsoft products, the wizard-based installs, minimum configuration, understanding the interoperability between all the other application stacks that we have on our desktops."

With the significant infrastructure investment in Microsoft already in place, Foster looked at RMS in Microsoft Windows Server 2008. He developed a high level design and set it up in the lab environment. "When we brought the RMS product in, we were already in the Windows Server 2008 TAP [technology adoption program], and we had previewed the beds and had the support we needed for a proof of concept implementation. It was like night and day on the implementation side, and this was with a beta product," Foster notes.

From the start, the engineering side of the RMS implementation was smooth, which has a major impact on the total cost of ownership, since engineering time can quickly add up. "We always look at the cost of implementing a project year over year, since that is one of the key costs, along with operational considerations," says Foster, "and implementation costs for RMS were significantly less." One of the key benefits with RMS was out-of-the-box integration with Active Directory (AD), a necessity since applying rights-based policies relies on AD users and groups. The Technology Unit was able to take advantage of the high availability configuration of their domain controllers and not introduce any single point of failure. "As an engineer I try to design solutions that don't have those types of operational requirements or relationships, but rather I want to decouple operations as much as possible, so that when I have an operational issue, it doesn't impact my line of business applications," says Foster.

The Technology Unit at Continental Airlines undertook the RMS Server project in the early part of summer 2007, at which time the HR and Legal Units bought in. By August,

the proof of concept had turned into a pilot implementation with much more of an enterprise scope with a hundred users mixed across four business units. The RMS solution from Microsoft Windows Server 2008 performs much better in regard to the operational aspects of Active Directory because RMS doesn't tie to one Active Directory, but to the entire domain and/or forest of servers within which it is implemented. "When I talk about total cost of ownership," Foster explains, "the more transparent and robust connection between AD and the servers is another cost example of administration and communication costs being held in check."

Going Enterprise-Wide

"In the first quarter of 2008, we're doing the production deployment with a scope of 500 users initially," says Foster, "but we all understand that as soon as this gets out it is going to be one of those snowball-type technologies where the word spreads socially—at lunch time you're talking about it, someone catches you in the hallway, or you get a document that has rights management applied to it and you've never used it before, and become an adopter." Foster predicts that within a year RMS is going to go to every desktop across Continental. "Every user that opens an email, every user that writes any type of document, whether it's an Excel document or a Word document or Visio, or as a PDF," he says, will expand the use of RMS. The Technology Unit is looking at third party solutions that work closely with Microsoft to provide PDF rights management through the RMS solution, so that the initial impetus for rights management will be covered.

Continental Airlines has nearly 200 Active Directory domain controllers across the specifically for rights management they are using Microsoft clustering services with the database for rights management in a cluster to provide high availability. On the front end of operations, Continental Airlines has redundant RMS servers split out into three different roles, with those roles segmented into multiple physical servers.

The Technology Unit is also looking at implementing RMS license pre-fetching with Microsoft Exchange 2007 to provide improved performance for rights protected email. "Understanding how the RMS design works is instrumental in putting together an architecture that is globally flexible without causing negative impact to the user," notes Foster, "and that's where the Exchange caching-type solutions come in. As part of this we are implementing a migration from Exchange 2003 to Exchange 2007 that will precede the global implementation of RMS."

Part of the global rollout of RMS means looking for wider application of the technology among the business units. "We've gone to 90% of our business units with RMS," says Foster. "One example is the business unit that handles the maintenance of aircraft, called the Technology Operations Unit. This unit has a FAA bulletin process that requires the mechanic to sign off on specific documents, which we have to track, noting that the mechanic reads it, and so forth, in a specific chain of custody of the document." The existing solution for this business unit is Documentum-based, which has been doing "chain of custody"-type management. But the Technical Unit wonders about the consequences of the momentum RMS is expected to gain when it goes enterprise-wide. "As the passion spreads about what RMS does and how it works and what it can do for

you, then it is going to result in reverse adoptions," believes Foster. "Instead of us going to them, it will be them coming to us, saying we can use this enterprise solution instead of our current business unit solution for the bulletins from the FAA and the bulletins from Boeing around parts and maintenance changes, all that kind of thing." Foster's team also went to the Flight Operations business unit that deals with pilots and flight attendants, where pilots, for example, have to go through a certain amount of training and need to show that they've completed it.

Part of the Technical Unit's discussion with the Legal Unit involves the issue of compliance, whether in terms of Sarbanes-Oxley (SOX), or Payment Card Industry Data Security (PCI), or the many other corporate standards that have to be met and audited against. Since one result of RMS is the ability to show not only who can open a document but also who actually has opened that document—what is often called usage tracking—RMS is seen as supplying the means to meet those requirements.

The Technical Unit hasn't kept itself out of the RMS discussions. They use a Microsoft SharePoint portal through which all architecture-type documents and projects are stored and shared in the process of reviewing and approving their efforts. "One of the values that RMS brings our own business unit is in terms of review," Foster says, "with the idea that if I'm creating a document on a design proposal, what RMS allows us to do is to designate the specific people in my peer review circle who should be looking at the document, but also to create an accountability, where I can know who specifically went to the document and reviewed the document because I see a tracking." Furthermore, once the document has gone through this peer review process and been approved, the document's originator or manager will know whether the document has been changed and who did edits. While some of this sort of thing can be done with Active Directory today, with RMS there can be more sophisticated control and tracking of documents, changes, and usage.

"This is going to be a watershed technology," says Foster, who likens RMS to other key business technologies like email, universally adopted throughout the years, or like the ubiquitous use of the Web browser by business today. "I believe that RMS is going to be another fundamental technology that everyone uses, and not thought of as a separate application. It is like Active Directory—it is just there and everyone uses it," claims Foster. "I don't need to know what server I just got my tickets from and all the details of the technology, but only that its there, it works. That is what RMS is going to become."

The User Experience with Microsoft RMS

Having a robust architecture for managing and serving rights is all well and good, but what can be done with it depends, in the end, on people setting policies and assigning rights. How do the managers find setting policies and assigning rights with the Microsoft RMS solution? The answer, for Continental Airlines' Technical Unit, is to provide a flexible design that is able to give different capabilities to business units that may have different requirements or even styles of management. Within the current pilot implementation, for example, the Financial Unit is concerned with a relatively small set of documents, and has one person who decides on and assigns document rights, while over at HR everybody in that business unit assigns rights to documents.

The flexibility comes through security groups in Active Directory and thereby offers the ability to apply rights across an entire business unit or through individual assignments of rights. "I don't want to spend a whole lot of time understanding your specific business requirements in order to enable you to use RMS," notes Foster. "If you have additional requirements, you come to us and we can look at ways of helping you understand the architecture so that you'll know how to implement it on a group level, or on a business unit level."

A core factor in the RMS implementation's flexibility is Continental Airlines' synchronizing their HR database with Active Directory. Every night, the HR system is tied directly to Active Directory, so that every employee and the particular business unit they are in, along with lots of other information, is updated. "The beauty of this," says Foster, "is if people move within the Continental framework or they leave the company, come into the company, or whatever happens from an employment perspective, all of that is captured in our Active Directory. We can then easily apply policy and/or rights based on who you report to, what business unit you report to, and your cost center information," which at Continental Airlines links funding, cost entries, and accounts to individuals and business units, with these links also stored in Active Directory.

In practice, this means that if rights are applied to a document that permits access only to HR employees, then the day an HR employee switches to a different business unit, the change is noted and automatically the employee no longer has HR-related rights. For Foster, it is the concept of the living document that comes into play, where today one may have a specific set of rights, but if those rights assignments change—say with a transfer to a different business unit—so changes the access to the document. "This was the sort of thing that HR was very interested in," Foster notes.

Being able to meet requirements is, of course, not necessarily the same thing as being easy to use or transparent to the end-user. Much of the discussion of both consumer- and enterprise-oriented digital rights management (DRM) has rightly focused on DRM's impact on the end user. "Any time enterprise engineering adopts a technology," reports Foster, "we have accountability to the enterprise to provide operational guidance, and we have responsibility toward the users for guidance." The Technical Unit creates a document for the help desk that outlines the functions and processes, so that if a user calls the help desk, the user gets help. In addition, the Technical Unit is in the process of writing a user communication that informs recipients about having specific rights, the abilities these rights provide, and the requirement of the recipient relevant to certain document types. These user communications also include a "how-to" tutorial in the form of screen shots and point and click guides that show exactly what to do to apply the rights, or to forward or edit the document, or whatever else may be specified with RMS. "We're working closely with the business units to create these how-to documents," says Foster, but in addition to this support, some of the business units are also producing official communications that get sent to everyone in the business unit about RMS and what is expected with RMS. Continental Airlines' Technical Unit is basically adding technical documentation, help functions, and rights policy documentation support so that from the line of business point of view, the RMS implementation is that much easier.

The concern about the interface for policy makers and end-users of RMS may be easily overstated, according to Foster. "From a policy perspective," he says, "you will see a subset of users who will define RMS policy, and a small subset of actual users who will create the policies for any particular business unit or division." The majority of end users behave no differently than their colleagues, applying policy to their own specific documents not based on a policy from their business unit, but simply on the way they control who can read the email, print the document, or other "on-the-fly" requirements chosen. "What you're going to see is four or five business unit policies that they'll have to apply," says Foster. "But what is likely is that the end user will apply some policy to documents every day, once RMS is made available. It is like an email—you address it specifically every time you send an email, and I think that it will become every time you send an email, you are not only going to say who you want it to go to, but now also who you don't want it to go to." In terms of rights policies, only a few are likely to define them, but from the end-user perspective, RMS is going to get used a lot, Foster believes. "I really think that the enabling of the end user for rights is going to be just as native as defining the 'TO:' field in email."

One reason for Foster's view on ease of use is that RMS is integrated within the user interface in Microsoft Office 2007 as point-and-click pull-down menu options on virtually every desktop within Continental Airlines. "RMS is right there in the title bar, and there is no launching of a third-party tool," he notes. With RMS integrated into MS Office, barriers to adoption are less likely, Foster argues, because "the end user is enabled now, and we're taking the power and capabilities of this rights concept and we're pushing it all the way down to the people who are actually opening and saving files, creating the intellectual property at Continental Airlines."

Conclusion: Unexpected Value

RMS implementation within Continental Airlines is still in early stages, just coming out of pilot program and there hasn't been a lot of "water cooler talk" about it yet. "I'll tell you this," Foster admits, "if RMS wasn't meeting the core business requirements, I would know about that. The fact is that 'no news is good news' applies, but within another three or four months we'll be getting the water cool talk and the little stories here and there about how this technology brings us additional value that we didn't even see initially."

III. Directory of ERM Solutions

The following companies develop and market software technologies for enterprise rights management. Sponsors of the research underlying this report are indicated by their logos and by additional product and market details in their entries. All product names are trademarks or registered trademarks of their respective owners.

Adobe Systems, Inc.

345 Park Avenue
San Jose, CA 95110 USA
http://adobe.com

Founded 1982, public (NASDAQ:ADBE)
Sales phone (US): (888) 649.2990
Sales email: contact Adobe sales representative

Products: Adobe LiveCycle Rights Management ES

Avoco Secure Ltd.

8 Clifford Street
London W1S 2LQ UK
http://avocosecure.com

Founded 2006, private
Sales phone (US): +1.415.839.9433
Sales email: sales@avocosecure.com

Products: secure2trust, secure2sign, secure2email

EMC

EMC²
where information lives®

176 South Street
Hopkinton, MA 01748 USA
http://emc.com

Founded 1978, public (NYSE:EMC)
Sales phone (US): (800) 607.9546
Sales email: softwaresales@emc.com

Products: EMC Documentum IRM Product Suite

Vertical markets: All

Operating systems: Microsoft Windows, Sun Solaris, Apple Macintosh

Content type support: Multiple types, extensible via SDK

Fasoo.com

17th Fl., Business Center, Nuritkum Square, 1605 Sangam-dong, Mapo-gu
Seoul, Korea (121-270)
http://fasoo.com

Founded 2000, private
Sales phone: +82.2.300.9102
Sales email: inquiry@fasoo.com

Products: Fasoo Secure Document, Fasoo Secure Node, Fasoo Secure Exchange, Fasoo Secure Web, Fasoo Secure Print, Fasoo Secure File-server, XDRM, XDRM-W

Solutions: DRM ONE for Enterprise, DRM ONE for Professionals, DRM ONE for SharePoint

Vertical markets: Covers all vertical markets (Public Sector, Education, Manufacturing, Construction, Medical/Healthcare, Petro-Chemical, Telco, Finance, Logistics, Engineering, Service and everything in between and beyond)

Operating systems: Fasoo DRM Server supports Windows 2000 Server (SP4 or higher), Windows Server 2003 (SP1 or higher), HP-UX (11 or higher) , SunOS (5.6 or higher), AIX (4 or higher); Fasoo DRM Client supports Windows 2000 Professional, Windows XP, Windows Vista (32bit)

Content type support: Supports most file types and applications (MS Office/ Notepad/WordPad/Project/Visio, Adobe Acrobat Standard/Reader/Distiller, Adobe Photoshop/Illustrator, MS Paint, AutoCAD, CATIA, Ideas, ProductView, SolidWorks, OrCAD, Unigraphics, 3D MAX and all the other 3rd party applications)

GigaTrust

607 Herndon Parkway, Suite 302
Herndon, VA 20170 USA
http://GigaTrust.com

Founded 2000, private
Sales phone: (866) 868 7878
Sales email: sales@GigaTrust.com

Products: Intelligent Rights Management, GigaTrust Enterprise Plus, GigaTrust for Blackberry, GigaTrust eDiscovery Agent, GigaTrust Dynamic File Folder. Offered through acquisition of Pinion Software (2008): ShareSafe Desktop, ShareSafe SDK, Pinion Receiver, Pinion Sanitizer.

Vertical markets: Financial Services, Manufacturing, Health Care & Public Sector

Operating systems: Microsoft Windows Server 2003 & 2008 with Microsoft Rights Management Services (RMS), Windows XP and Vista, BlackBerry

Content type support: Email, Microsoft Office Suite, PDF files, Microsoft VISIO, Microsoft Project, HTML, image files, PTC ProductView, CAD

Liquid Machines, Inc.

100 Fifth Ave., 5th Floor
Waltham, MA 02451 USA
http://liquidmachines.com

Founded 2001, private
Sales phone: (877) 885 4784
Sales email: info@liquidmachines.com

Products: Liquid Machines Document Control, Liquid Machines Email Control, Liquid Machines Workgroup Editions, Liquid Machines Gateway for Blackberry, Liquid Machines Fileshare Gateway, Liquid Machines for SolidWorks, Liquid Machines Google Mini Gateway

LockLizard

Longlands Park
Ayr, KA7 4RJ Scotland
http://locklizard.com

Founded 2004, private
Sales phone (US): (800) 707 4492
Sales email: sales@locklizard.com

Products: Lizard Safeguard, Lizard Protector, Lizard Guardian

Microsoft

1 Microsoft Way
Redmond, WA 98052-6399 USA
http://microsoft.com

Founded 1975, public (NYSE:MSFT)
Sales phone: (800) 426-9400
Sales email: http://www.microsoft.com/licensing/default.mspx

Products: Windows Server Active Directory Rights Management Services (AD RMS)

Vertical markets: All

Operating systems: Windows Server 2003, Windows Server 2008

Content type support: Email, documents, HTML/web pages

Modevity

Goshen Executive Center
1450 East Boot Road
Building 400, Suite C
West Chester, Pa 19380
http://modevity.com

Founded 1977, public (NASDAQ:ORCL)
Sales phone: (610) 738 9700 ext. 119
Sales email: sales@modevity.com

Products: Imperium

Oracle Corporation

500 Oracle Parkway
Redwood Shores, CA 94065 USA
http://oracle.com

Founded 1977, public (NASDAQ:ORCL)
Sales phone: (800) 633 0738
Sales email:

Products: Oracle Information Rights Management

Vitrium Systems, Inc.

502-1168 Hamilton Street.
Vancouver, BC, V6B 2S2 Canada
http://vitrium.com

Founded 2005, private
Sales phone: (866) 403 1500
Sales email: sales@vitrium.com

Products: Protectedpdf, Docmetrics

Workshare, Inc.

208 Utah Street, Suite 350
San Francisco, CA 94103 USA
http://workshare.com

Founded 1999, private
Sales phone: (888) 404 4246
Sales email: sales@workshare.com

Products: Workshare Professional, Workshare Protect, Workshare Protect Network, Workshare Management System, Unified Content Protection Suite 6

IV. ERM Vendor Vision Statements

Fasoo.com

- Every business application will incorporate Enterprise DRM, as the digital business environment continues to evolve.
- Enterprise DRM will be an indispensable part of business applications as RDBMS and Web Server are today.
- Fasoo.com will be the leading innovator on Enterprise DRM Technology to be used for any content in any environment.
- Fasoo.com's products and services will be the core infrastructure of every organization and individual for the unimpeded secure distribution of digital content.

Kyugon Cho, Founder, President and CEO of Fasoo.com

GigaTrust

GigaTrust seeks to increase the value of enterprise rights management for governmental organizations and corporate enterprises and ease the enforcement of policy in the process bringing security to their business relationships and processes. GigaTrust is focused on helping our customers leverage enterprise rights management technology to build secure communication and collaboration environments for their organizations and their business and supply chain partners. The interest in ERM solutions is growing rapidly for a number of reasons.

Many organizations have taken steps to enhance their perimeter and network. They have updated firewall technology, implemented role based access control; they are using file and whole disk encryption, and deployed email encryption gateways/tunnels. This is usually referred to as protection In Transit and At Rest. However the reality is that for organizations to do business they need to be able to exchange information securely with internal employees who are mobile, as well as with external business and supply chain partners and customers. This ordinarily takes the form of documents and email and frequently these communications contain sensitive information. Companies have now come to realize that they need to protect these documents while In Use and that is where ERM comes in. Two other major reasons we see increased interest in ERM revolve around the intellectual and compliance content of these communications themselves.

Intellectual Property: Many companies now recognize that they are in the intellectual property business. They understand that these documents contain their R&D and design work, strategic planning ideas, and proprietary methods they use to serve their customers. Losing control of that information would constitute losing control over their corporate assets.

Compliance: The information in many of these corporate communications is frequently subject to regulation based on governmental oversight or corporate governance policy. Certain types of documents and communications can only be shared with specific individuals and protected from all others.

The GigaTrust Intelligent Rights Management© solutions build on top of the Rights Management Services (RMS) platform from Microsoft. We chose to work with RMS because we saw the opportunity to add value to a pervasive platform allowing customers to leverage existing internal processes without forcing them into a proprietary software platform that would necessitate changes to their work flows.

GigaTrust solutions allow organizations to automate policy enforcement and quickly and easily include their supply chain and business partners in a secure communication ecosystem. We extend the security of RMS to the corporate BlackBerry users enabling secure mobility for corporate executives or first responders in the government. GigaTrust also focuses on sensitive information in graphical form—CAD and

engineering drawings—which for many companies represents the core of their intellectual property. We make it possible for manufacturers and others sharing CAD drawings to do so securely while insuring that only the right partners or customers get access to sensitive product representations.

Brad Gandee, Vice President Product Marketing and Management, GigaTrust

Microsoft

Enabling Identity-Based Information Protection in a Connected World

As more and more of the world's information, commerce, and communications moves to digital form, it will open the door to a new world of connected experiences that link our interests and our communities into a seamless whole that extends across home, work, school, and play.

Increasingly, people envision a world of anywhere access—a world in which the information, the communities, and the content that they value is available instantly and easily, no matter where they are.

Of course we're not quite there yet. But whether we get there or not is no longer a question of the power of our devices and the speed of our connections. The real issue today is security. Ultimately, anywhere access depends on whether we can create and share information without fear that it will be compromised, stolen, or exploited.

The answer lies in trust—in creating systems and processes that are always secure so that people and organizations have a high degree of confidence that the technology they use will protect their identity, their privacy, and their information. This is an imperative that transcends any one company. Success will require hard work and extensive cooperation between companies, governments, and organizations from around the world.

Achieving the levels of trust needed to make connected experiences based on anywhere access possible will require a change to the way we approach digital identities, build networks, and protect information.

The Evolution of Information Protection

It is impossible to overstate the importance of providing the right levels of privacy and information protection so that people can trust that their information is secure. To achieve this, we must be able to protect information not only when it is in transit, but also on the server, the desktop, mobile device, and wherever else it may reside. Policy plays an important role in the evolution of protection. By applying appropriate policy when information is created and throughout the information lifecycle, we can enable information to flow freely and safely across systems and networks while maintaining appropriate control over how it is used, and by whom.

Weaving together the notions of identity, trust, and policy is a critical step in the evolution of information protection. Trust relationships must be established not only between people within the same organization, but also across organizations with a wide variety of technology infrastructures.

Federation is at the center of getting all of these trust connections to work. The standards around Web services are an important milestone and make it possible for people to work with outside organizations in a very secure way. Federation service-enabled applications leverage established relationships to enable secure collaboration with external entities. For example, an organization that has deployed Windows Server® 2008 Active Directory Rights Management Services (AD RMS) can set-up federation [using AD Federation Services] with an external entity and leverage the relationship to share rights-protected content across the two organizations without the need to manage external users within a local domain, or require a deployment of AD RMS in both places.

Microsoft is innovating across a wide range of products and technologies to continue the evolution of information protection using an identity-based approach. Examples include the integration of Rights Management Services (RMS) and Active Directory Federation Services (AD FS) enabling secure collaboration scenarios between organizations as well as the automatic application of RMS policy to documents stored in Microsoft Office SharePoint directories. We envision the transformation of the industry toward a seamless identity-based protection of information that works across the connected world and is enabled automatically throughout the entire information lifecycle.

Doug Leland, General Manager Identity and Security Business Goup, Microsoft Corp.

EMC

Organizations have long valued EMC's Enterprise Content Management (ECM) capabilities for securing and managing all their unstructured content. The EMC Documentum suite of products has always ensured that people can only access content to which they are authorized. When customers began asking for ways to extend their document protection beyond the corporate firewall, we added Information Rights Management capabilities to our product suite. Information Rights Management gives organizations the ability to retain control of their confidential information regardless of where it travels or is stored.

Organizations across all industries work with confidential documents vital to their business. Whether it's intellectual property, government secrets or personal information of customers, EMC is able to secure and protect critical information persistently throughout its life. And, as the value and use of information changes throughout its lifecycle, the rights to access protected information can be changed or revoked at any time, no matter where the content resides. The importance and security needs of content change over time. The dynamic nature of IRM policies are a natural fit with the content management concept of Information Lifecycle Management.

Rather than using such technology only for small projects or point solutions, EMC foresees the need for organizations to protect their content at all levels of the enterprise. Now that the technical barriers to wide-scale deployment have been overcome, organizations can easily deploy IRM within solutions across the enterprise, ensuring protection for content authored anywhere in the organization. In its nascent stages, information rights products were difficult to deploy at the enterprise level due to a myriad of problems from authenticating external users to determining which documents required protection. Over the past few years, this has rapidly begun to change. Through integration with content management, organizations are now able standardize their protection practices and automatically protect critical documents based on pre-defined policies and any of the rich metadata captured in such a system.

The uses for rights management can also extend beyond security. Take, for instance, the core content management capability of document versioning. Typically content management systems allow users to version a document but do not ensure that only the latest version of a document is used, since older versions are often in circulation beyond the reach of the content management system. IRM can be used to enforce good business practices by automatically expiring old content, making legacy files inaccessible irrespective of where those files reside, and requiring people to access the current version for use

A final obstacle faced by many organizations is the protection of sensitive information that already exists throughout the company. This is a key part of the future for Information Rights Management. EMC's RSA division is a leader in Data Loss Protection (DLP). DLP technology gives organizations the ability to scan the entire

information infrastructure and identify sensitive information. Combining this technology with Information Rights Management is extremely powerful, providing the ability to both identify and persistently protect sensitive information throughout the organization. IRM integrated with DLP will provide an end to end solution for discovering and securing sensitive information throughout the enterprise.

Balaji Yelamanchili, Sr.Vice President and General Manager, EMC Content Management & Archiving

Project Team

The program lead is **Bill Rosenblatt, Senior Analyst, Gilbane Group, and President, Giant Steps Media Technology Strategies.** He is a recognized authority on digital media technologies, including digital rights management, content management, cross-media strategy, and content production systems, as well as on issues related to intellectual property in the online world. Bill is the managing editor of the e-newsletter DRM Watch (www.drmwatch.com), and author of Digital Rights Management: Business and Technology (John Wiley & Sons, 2001) and Digital Rights for Digital Television (in Television Goes Digital, Springer-Verlag, 2008) as well as several white papers on digital rights technologies. Bill has consulted on digital rights technologies for a wide range of content providers, technology vendors, and public policy entities around the world.

Bill Trippe is Senior Analyst, Gilbane Group, covering trends and technologies in the content management industry, and **President, New Millennium Publishing**, a consulting company that helps publishers make the best use of content management and publishing technology. Bill has more than 20 years of technical and management experience in content management and publishing technologies for print and multi-channel output. Clients include major companies where publishing is the core business and where publishing is a demanding "second business." Bill is also co-author of Digital Rights Management: Business and Technology.

David Guenette is Associate Analyst, Gilbane Group, and Principle of DRG Publications, a practice covering the connected content market with strategic technology and business development research, analysis, and editorial content, with focus on both digital rights management and the editorial process within electronic publishing.

Mary Laplante is Vice President, Consulting Services, Gilbane Group. She oversees Gilbane's consulting practice, manages research projects, contributes editorial content, and participates in Gilbane conferences and other industry events. Mary has twenty-two years of experience in standards, publishing, software marketing, and research and consulting. She served as project manager for the study program.