

Information Management and Your Corporate Reputation

Summary

Trends

The landscape of information management is changing as a result of several long-term trends. Existing and emerging laws and regulations result in a challenge to ensure compliance. Changes in litigation risk are resulting in more lawsuits and earlier, higher settlements. Technology strategies, traditionally focused on operational and storage issues, may not be in alignment with records management requirements, resulting in higher discovery costs and risks. In addition to these trends, several current “triggering” events are shining a spotlight on records management and forcing a redefinition of the challenges and solutions. The bottom line is that records management has moved from operational obscurity to headline news and is now a major factor in your corporate reputation.

Meeting the Challenges

To meet the challenges, organizations must develop and support effective retention programs. The ultimate vision is to enable a universal archive for an organization, but the reality is that companies must work within technical and operational limitations to balance trade-offs and develop a phased approach.

Building an Effective Retention Program

The elements of building an effective retention program include designing for consistency and usability, implementing and supporting an organization-wide program, and auditing and updating the program to ensure currency and compliance.

In the End

Once you understand the trends and the vision for the optimal records management program, you can begin to build an effective retention program. The benefits will be improved compliance, reduced litigation costs, lower cost of records storage, easier access to information, and an improved “good faith” corporate image.

EFFECTIVELY MANAGING RISK FOR YOUR ORGANIZATION REQUIRES UNDERSTANDING THE TRENDS AFFECTING INFORMATION MANAGEMENT AND THEIR RESULTING CHALLENGES. THREE MAJOR, LONG-TERM TRENDS ARE CHANGING THE LANDSCAPE OF INFORMATION MANAGEMENT. IN ADDITION, THERE ARE SEVERAL “TRIGGERING” EVENTS THAT ARE RAISING THE STAKES AND FORCING ORGANIZATIONS TO REDEFINE THE INFORMATION MANAGEMENT CHALLENGES AND EVOLVE BETTER RECORDS MANAGEMENT SOLUTIONS.

Trend: Existing Laws and Regulations

There is an expanding body of legislation and compliance requirements mandating how and when certain types of information may be used, stored, retained and destroyed. These regulations result from a variety of trends and factors.

Certain industries have regulations mandating how information must be stored and made available, such as SEC Rule 17a-4 for broker-dealers. The Internet boom has produced a spate of privacy laws—such as Gramm-Leach-Bliley, HIPAA, and a variety of state laws—regulating access to personal information. In response to the recent corporate ethics crisis, the Sarbanes-Oxley act adds a new dimension to the emerging legal landscape; in addition to creating a new set of auditor independence rules and new disclosure requirements for public companies, the Act increases maximum fraud penalties and imposes new certification responsibilities on CEOs and CFOs, exposing them to greater potential liability. (See sidebar *Overview of Selected Regulations*.)

In addition to passing legislation, regulators are responding to public pressure for compliance. For example, with the recent increase in investigations into corporate accounting practices, the SEC has fined six top investment houses on Wall Street over \$10 million for failing to keep e-mails in compliance with retention regulations. This trend is likely to continue as confidence in corporate ethics remains low and the pressure to audit compliance remains high.

Result: Compliance Challenge

Complying with the panoply of legislation can be a challenge. There are federal and state laws as well as industry-specific regulations that mandate who may access information, how information may be accessed, where information may be stored, how information may be stored, how long information must be retained, when information may be destroyed, and how information must be delivered in the event of an audit or litigation. Combined with the explosion of information and the inherent limitations in technology and operational requirements, this can be a daunting task. Organizations are looking to new technologies and information management approaches to help meet this challenge.

Overview of Selected Regulations

Following are highlights of several regulations that affect how information is managed:

- **SEC 17a-4**—Specifies the requirements to which broker-dealers must conform for keeping and retaining electronic, micrographic, and paper client correspondence. Specifically, the Rule details not only what records may be retained electronically, but also how electronic records must be stored and maintained.
- **Gramm-Leach-Bliley (GLBAA)**—Requires that all financial institutions disclose their policies and practices for protecting the privacy of non-public, personal information of their customers. The Act allows for the affiliation between financial institutions and the sharing of customer information among affiliates; however, the customer has the opportunity to decline the sharing of non-public personal information with non-affiliates.
- **Healthcare Information Portability and Accountability Act (HIPAA)**—Intended to protect medical records and other health information held or disclosed by covered entities, and includes requirements to issue regulations related to the privacy of patients' health information.
- **Sarbanes-Oxley**—Protects investors by improving the accuracy and reliability of corporate disclosures made available under the securities laws. The Public Company Accounting Oversight Board, a nonprofit corporation consisting of non-government affiliated members, was established to oversee the audit of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies.

Trend: Changes in Litigation Risks

In addition to emerging legislation, other changes in the litigation landscape are shifting the risks facing companies. For example, the explosion of information increases both the cost and risk of discovery. This is compounded by Rule 26 of the Federal Rules of Civil Procedure which shifts the discovery burden onto the defendant (see sidebar *Implications of Rule 26*).

The boom in electronic information has also raised the risk element. According to IDC, there were 47 million business e-mail users in North America in 1995; that number shot up to 190 million in 2002 and is projected to go up to 220 million in 2005. The average number of e-mail messages sent daily has similarly exploded from 200 million in 1995, to 6.8 billion in 2002, with an outlook of 10.5 billion in 2005. This growth significantly increases the volume of potentially discoverable information that must be produced, as well as the cost of producing that information.

Electronic information tends to be managed by *format* not *content*; it is usually stored and backed up with the application that created it, resulting in information silos. Discoverable information, however, is identified by content. Therefore, finding all information relevant to a disputed issue can mean locating records in multiple systems or applications, such as e-mail systems, financial applications, or HR systems, for example.

Electronic information—especially e-mail—is often treated more casually than other documents, increasing the risk exposure. Sophisticated computer forensics technologies and capabilities also increase risk; data that has been properly purged from an IT perspective may still be discoverable because records retention policies and practices are not part of that process.

Result: More Lawsuits, Higher Settlements

With Rule 26, the cost threshold to initiate suits has gone down, which increases the potential for lawsuits to be initiated. Defendants who lack trust in their information management systems may rush to an early settlement, possibly even agreeing to a higher settlement than they would otherwise, to avoid exposing themselves to the cost and risk associated with the discovery process. Both of these factors can lead to an increase in lawsuits.

Implications of Rule 26

Prior to Rule 26 of the Federal Rules of Civil Procedure, the burden was on requestors to identify relevant records, request the records and, in some cases, subpoena records. Rule 26 stipulates that each party involved in litigation must proactively provide a description of all records relevant to the disputed facts without waiting for discovery requests. Specific requirements of the Rule include:

- Contact information of each individual likely to have discoverable information
- A copy or description (including category and location) of all relevant information
- Delivery of the above information within specified time frames (within approximately 85 days from the time the defendant files an answer and 90 days before trial)

The objective of Rule 26 was to accelerate the exchange of information during the pre-trial process by eliminating the information-request paperwork to combat the long and difficult discovery process that had, in some cases, prolonged federal cases for years. The result is that organizations with poor records management programs will find it difficult to comply and may face sanctions or loss of rights.

Trend: Impact of Technology

With the emerging importance of electronic information in litigation, technology plays an increasingly responsible role in risk management. But traditional IT architectures and processes are not designed to manage litigation risk.

Applications are designed for broad operational use and access to information, not for retention, legal discovery and low-cost records archiving. Systems are designed for managing transactions and storing transactional data. Traditional IT systems treat data and records alike (see sidebar *Data vs. Records: What's the Difference?*), information is stored in application silos, and backups function as the official archive. IT storage management strategies also focus on recovery. The inclination is to keep information forever (managing disaster recovery risk), not to apply retention management policies and procedures to backup and recovery processes (managing legal risk). As a result, managing, identifying and delivering information from applications and systems for discovery can be difficult and costly.

Result: High Cost, Poor Image

When backups are used as archives (see sidebar *Backups vs. Archives: What's the Difference?*), the cost of discovery can be significantly higher. Backups are designed to restore entire systems and locating unindexed individual records from backups is difficult and expensive. Because the tendency is to hoard information rather than purge based on retention policies, there is increased volumes and, hence, cost. As a result, organizations may have a hard time responding to discovery and risk uncovering “surprises.” Delays and other problems encountered as a result of these difficulties may be interpreted as bad faith.

Data vs. Records: What's the Difference?

Not all data are records. Records represent the official record or sole copy of a document that needs to be archived. Records have evidentiary value and legal credibility; not all data meets evidentiary standards. Data that are not records should be purged through routine destruction processes according to your organization's retention policies. Examples of data that should be considered records include:

- A job offer sent to a prospective employee where the document is the official offer
- A contract negotiation containing finalized agreed-upon pricing
- A memo sent to employees informing of a new policy or process

Examples of data that should not be considered records, and that should be purged, include:

- Drafts of documents or in-progress discussions/negotiations (only the final communication should be considered a record)
- Received copies of records; for example, in the case of a policy memo sent to all employees, only the original memo sent must be archived—the copies received by hundreds or thousands of employees do not also need to be archived as records
- Miscellaneous communications such as meeting requests, project coordination, lunch plans, etc.

Backup vs. Archives: What's the Difference?

Both activities relate to storing electronic data, but the fundamental difference between backup and archiving is reflected in the answer to the following question: For what purpose are you storing the data?

- If you are storing data for the purpose of recovering systems from a disaster, crash or data corruption, you are performing backup
- If you are storing data with the expectation that you may need to use or access individual records in the future for business operations, you are archiving.

All electronic data should be backed up. Not all electronic data need to be archived. In some cases, there are regulations requiring that certain types of data in certain industries be archived. Some regulations even provide specific archiving method requirements.

Events Triggering a Redefinition of the Problem

These trends are long term and have emerged over several years. There are, however, specific events—including the recent accounting scandals, alleged destruction of evidentiary documents, and the corporate ethics “crisis”—that have an immediate impact and are forcing a redefinition of the information management challenges and solutions. Records management has moved from the back room to the board room. No longer just an operational function, the records management discipline has become a strategic risk management imperative. The risks of poor records management are significant—lax records management practices can be reflected as unethical corporate behavior which can lead to adverse judgments, executive personal liability, increased risk costs, and lower stock prices due to lack of trust.

THE KEY TO MEETING THE NEW RISK-MANAGEMENT CHALLENGES IS TO HAVE AN EFFECTIVE RECORDS RETENTION PROGRAM THAT BALANCES THE NEEDS FOR TIMELY ACCESS TO INFORMATION FOR REFERENCE (DAILY OPERATIONS) AND DEFENSE (LITIGATION), MEETING COMPLIANCE REQUIREMENTS, MEETING EMERGING STANDARDS OF "REASONABLENESS" AND GOOD CORPORATE CITIZENSHIP, PRESERVING THE ORGANIZATION'S HISTORY, AND MANAGING COSTS. IT IS IMPORTANT TO UNDERSTAND BOTH THE ULTIMATE VISION FOR A RETENTION PROGRAM AS WELL AS EXISTING LIMITATIONS. BY KEEPING AN EYE ON THE VISION WHILE IMPLEMENTING PRACTICAL SOLUTIONS AND IMPROVEMENTS, ORGANIZATIONS CAN START ON THE PATH TO MEETING THESE CHALLENGES.

The Vision

The brass ring of records retention is the concept of a universal archive that identifies records (as opposed to data), applies classification by content, enables search and retrieval for both reference and litigation purposes, and effectively destroys records based on the corporate retention policy. There are no information silos and all information requests are made purely based on content, irrespective of format or the operational system it resides in.

The next section discusses the elements of an effective retention program and the considerations that need to be made to ensure that the benefits of lowered risk, lowered cost, and improved corporate image are realized.

Today's Reality

Unfortunately, this vision cannot practically be realized today. A variety of technical and operational challenges must be resolved before a universal archive can be a reality, especially within complex organizations. Companies should, however, begin looking for practical ways to achieve their records management goals. A targeted, phased approach will help companies make strides by enabling decisions that balance risk management with technology and operational capabilities. Many companies are starting this process by targeting high-exposure applications such as e-mail. E-mail is a universal communications medium that generates enormous volumes of data, is susceptible to the "casual use" phenomenon, and is a proven litigation risk—it is a prime candidate for immediate attention that can result in early gains in lowering risk and costs. Other appropriate areas to consider for phase-one implementation include customer communications such as electronic statements, and R&D records.

RECORDS MANAGEMENT HAS BECOME ONE OF THE VARIABLES THE MARKET USES TO ASSESS A COMPANY'S TRUSTWORTHINESS. THE BEST WAY TO ENSURE HIGH TRUST MARKS FOR THAT VARIABLE IS TO ENSURE THAT YOU HAVE AN EFFECTIVE RETENTION PROGRAM IN PLACE. THE GOALS OF A RETENTION PROGRAM ARE TO ENSURE COMPLIANCE, SUPPORT LITIGATION, AND REDUCE THE VOLUME OF RECORDS STORED. IN SHORT, YOU WANT TO MAKE YOUR RECORDS MANAGEMENT EFFORTS CONSISTENT, KEEP WHAT YOU NEED, DISPOSE OF THE REST, AND KEEP COSTS IN CHECK. TO ENSURE EFFECTIVENESS, YOU NEED TO FOCUS ON APPROPRIATE DESIGN, IMPLEMENTATION AND TRAINING, AUDITS, AND ONGOING UPDATES.

Design

The keys to effective program design are consistency, content, usability and compliance.

Ensure consistency across your entire organization. There are several levels of consistency. To ensure that the program's mechanics are consistent, define common record classes for like functions across business units, using unique record classes for business-line-specific records. Look for opportunities to use system-driven processes to reduce the dependencies on individuals. Ensure that the program is being adhered to consistently as part of the ordinary course of operations.

Ensure that content—not format—governs and design for media-independence. Until the universal archive is in reach, you can take an application-specific approach for dealing with electronic information. Because applications tend to house related records with a more specific risk boundary, you can include electronic records in your retention program with a methodical and streamlined approach.

Ensure that you design the program for your users. You will rely on your employees to adhere to the program and the vast majority of them are neither lawyers nor retention experts. A common mistake companies make is to develop a legally valid program that is impractical to maintain. You can increase usability of the program by defining fewer, broader classes and by taking operational retention needs into consideration in addition to legal retention requirements and using

the greater of the two. The goal is to build an operational corporate program that fosters compliance without requiring significant changes in employee behavior or knowledge.

Ensure compliance by making it as easy as possible for your users. Technology can be used for policy distribution and maintenance, broad access to policies and procedures, user help, destruction process control, implementation of legal records hold, training in high turnover employee populations, and activity monitoring.

For large organizations, litigation is simply a way of business life. Yet most companies are reactive to the discovery process. Part of an effective retention program can include building a discovery response process into the program appropriate to your industry.

When designing a retention program, maintain a less-is-best philosophy and leverage common legal research to lower development and maintenance costs, and to ensure consistent judgment calls in implementation. While records relevant to a specific litigation claim need to be suspended from routine destruction processes, this does not mean that the company's entire retention program must cease. A "hold" process is needed to ensure that the right records are kept while other non-relevant records are processed routinely.

Implementation

A records retention program is just that—a program. This is not a policy-driven event geared to lawyers and compliance officers, but a company program that is consistently used and supported by employees across the organization. You need to plan for a comprehensive, company-wide roll out. This includes broad communication and training.

In addition to educating your employees on the “whys” of retention management, you need to reinforce your program. Make employees accountable for compliance. In addition to instituting accountability, many companies require written acknowledgement of retention policies, which can be done together with annual affirmations of the company's privacy policy. For this to be effective, the program must have support from senior management.

Audit and Update

To ensure the ongoing effectiveness of your retention program, you must reinforce your implementation through auditing, and reassess your design for currency. You can train your employees and hold them accountable for compliance, but unless you audit your retention program, you can't be sure of its success and consistency. You need to ensure that records are consistently scheduled for destruction and that they are actually being destroyed after release. In addition, you need to ensure that your retention program keeps pace with changes in regulations as well as with organizational changes. You should periodically review your retention schedules accordingly.

Ten Deadly Sins of a Corporate Records Retention Program

Corporate America has generally under-invested in the area of records retention. The vast majority of companies do not regularly destroy information, let alone implement a records retention program. Companies struggle in this area because their policies are not legally sufficient and/or they cannot be implemented. These 10 deadly sins emerge:

1. The retention schedule no longer reflects the changes to the company.
2. The retention schedule is not based on legal or regulatory requirements; citations do not exist to support the retention periods.
3. The retention schedule is out of date and no longer reflects the law.
4. Formal policies and procedures do not exist or are inconsistent across departments.
5. Retention schedules cover paper records but not all media.
6. No one is responsible for administering a company's record management program.
7. The retention policies are not integrated into a records management system that can “report” to companies when to destroy records.
8. Users are oblivious to records policies.
9. There is no effective review or audit process for approving records destruction.
10. Companies freeze all destruction during litigation because they cannot identify those records pertinent to the litigation.

In the End

The effort required to develop an effective retention program can be significant, but it pales next to the risks of not making the investment. Sloppy records management has become a major factor in corporate ethics and a poor company image can result in fines, sanctions, drop in stock price, executive liability and other risks. On the flip side, the benefits of effective retention can include easier access to information, lower cost of records storage, increased ease of compliance, reduction in litigation discovery costs, and an improved corporate image of good faith.

Other Resources

The following articles on retention programs and risk management are available in the Records Storage & Management area of the Resources & Information section on Iron Mountain's Web site at www.ironmountain.com:

- [Ten Deadly Sins of a Corporate Records Retention Program](#)
- [Corporate Records Retention Programs: Managing Risks While Controlling Costs](#)
- [Can Your Records Management Program Withstand Attack?](#)
- [Getting Records Management on the Audit List](#)
- [E-mail as Records](#)
- [Electronic Discovery](#)

About Iron Mountain

Iron Mountain offers a broad array of records management services for both paper and electronic records, including retention program development, implementation and support, and records storage and access. Iron Mountain's Web-based records management system supports retention management and delivers robust search and access capabilities for low-cost implementation and ease-of-use.

Iron Mountain also offers a range of information protection and preservation solutions including:

- vital records management
- secure shredding services
- healthcare records management
- film and sound preservation
- secure backup, vaulting and rotation of information
- disaster recovery services and business continuity consulting
- intellectual property protection

Contact Iron Mountain at (800) 899-IRON or visit our Web site at www.ironmountain.com.