This article was originally published in the Fall 2006 edition of The John Liner Review.

When Information Management Becomes Risky Business

WILLIAM MILLICAN

Information management has become an increasingly serious area of risk for organizations of all types and sizes. It is key to business continuity, regulatory compliance, and stakeholder trust. If it's not on your risk management radar screen, it should be.

There have been many cases in the last few years that illustrate the impact records and information management can have on an organization. For instance, Arthur Andersen's document destruction policy came into question — and court — and contributed to the company's fall from grace.[1] Morgan Stanley's inability to produce e-mail in a high-profile court case resulted in an adverse inference instruction and, ultimately, penalties of $1.45 billion.[2] Phillip Morris' failure to save e-mails per its own information-management policies cost it $2.75 million.[3] These are just a few examples worthy of note.

Of course, we must not forget Enron's impact on corporate governance and compliance. As a result of Enron's very public downfall, the investigations of Arthur Andersen, and the questions of public accountability, the U.S. government passed sweeping reform that affects companies in the United States and abroad.

Before discussing some of the information management reforms and their impact on corporate information risk, we should define compliance. Compliance is often thrown around as a catch-all for "playing by the rules." A company is faced with the task of compliance in many ways. It must comply with all governmental regulations and legal requirements. Beyond external regulations, companies must comply with their own policies with respect to information management. They must also, for example, adhere to the mandates set forth in their own policy manuals regarding the information they keep or destroy. These internal policies should be created with this in mind.

It's also important to have a working definition of a record prior to examining the risks of managing information. A record is defined as "recorded information, regardless of medium or characteristics, made or received by an organization in pursuance of legal obligations or in the transaction of business."[4]

Risks Linked to Management of Records

One such reform, the Sarbanes-Oxley Act (SOX), has put compliance center stage and helped focus attention on the importance of effective records and information management. SOX stipulates specific retention periods for certain records. This encompasses all types of records — including electronic records such as e-mail, instant messages, and voice mail. In short, companies that don't take seriously the need to retain and to be able to produce documents as required by law could find themselves facing heavy fines and their executive officers facing incarceration.

But compliance is not the only area of risk linked to the management of records and information. Privacy and data security are also potential vulnerabilities for organizations these days. Over the past few months, there have been numerous reports in the news about lost records and stolen or lost computers containing sensitive information.[5] These incidents have put several thousands of consumers at risk of identity theft and other misuses of personally identifiable information.

To protect their information, particularly sensitive records involving their customers, is an inherent responsibility of all organizations. This has become a serious enough concern that several bills have been introduced in the U.S. Congress specifically addressing this issue of data protection.

For Example, H.R. 4127, Data Accountability and Trust Act (DATA), seeks to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information and to provide for nationwide notice in the event of a security breach. The Data Security Act of 2006 (S. 3568) is listed as a bill to protect information relating to consumers and to require notice of security breaches, while S. 115, the Notification of Risk to Personal Data Act, is a bill to require federal agencies and persons engaged in interstate commerce that are in possession of electronic data containing personal information to disclose any unauthorized acquisition of such information.[6]

Given the proliferation of electronic information, especially the phenomenal growth of e-mail, compliance and data protection are issues that will not go away soon.

Information Risks Must Be Handled

The message is clear: The information a company is called upon to manage on a daily basis can put any organization at risk. It's imperative that an organization's risk management effort take this type of risk into account.

Unfortunately, many organizations lack effective policies and procedures for systematic control of recorded information. They may, therefore,

- store some records too long, not long enough, or not at all;

- prematurely destroy or retire certain vital records;
- lose information needed for proper SEC reporting; and
- fail to properly safeguard and protect information and records from hackers or unauthorized insiders.

All of these actions increase the risk of incurring penalties for noncompliance with recordkeeping regulations, suffering a tarnished reputation, and facing possible legal liability. On the other hand, solid records and information management (RIM) controls demonstrate vigilance and help satisfy compliance efforts pertaining to corporate governance regulations such as Sarbanes-Oxley. Proactive records-management processes also help reduce litigation defense costs with regard to expensive electronic discovery in litigation proceedings. They also demonstrate a prudent level of due care essential to mitigating corporate risk resulting from events that can lead to liability exposure.

It's up to the risk management team to identify the perils facing its organization and to implement measures to reduce or eliminate the potential losses. This means taking a proactive, forward-thinking approach that takes these information-management-related practices into account and creates a business model with improved data- and records-management processes.

What to Look For in a Records and Information Management Program

There are several elements of a records and information management program that the risk management team must consider in determining whether the organization is being adequately protected. A good place to start is with the organization's records and information management policy.

A RIM policy should address the issues of creation or receipt, use, modification, and disposition — i.e., the information life cycle — of records and information.

Creation and Receipt of Records

Organizations are learning that if there is better information classification and governance beginning when records and information are created, it is easier to manage the overall life cycle. This, in turn, reduces the risk to the organization.

A classification system is the starting point for information governance. In essence, it gives desktop users — who create and manage information on a daily basis — the tools to classify the information they're managing right at the source. Users would be forced, for example, to answer questions about the documents they are creating in order to help classify these documents within the organization's overall content management system. The answers to these questions, in addition to information that is created by the application, are hidden and ap-

pended to the documents permanently to help the organization manage the documents throughout their life cycle. *Metadata* is the term we give that "hidden" information about a record: who created it and when, versions, keywords, etc.

Metadata facilitates the classification of records and makes it easier for authorized people to retrieve needed information, which also lowers risk for organizations. Organizations that cannot produce and securely provide the right information at the right time to the right people can find themselves at great risk during electronic discovery — as the Morgan Stanley case mentioned above dramatically illustrates. Also at risk are organizations that spend a significant amount on research and development if they cannot make results accessible to product teams across the planet, around the clock. Inaccessible information leads to duplicated research efforts or delayed product time to market — and the risk of increased costs.

Metadata is also important to the correct classification of information that an organization *receives* — for example, invoices from suppliers or vendors. Just like information created by an organization, information it receives must also be correctly classified so it can be readily accessed and provided to the right people at the right time, and its management must also be governed by the organization's retention policies, regardless of the medium on which that information exists.

Use, Modification, and Movement of Information

The policy, having successfully addressed the issues of creation and receipt, should focus next on how the use, modification, and movement of records and information shall be governed and managed.

Managing this portion of the life cycle is best handled by automated systems that work in an orchestrated fashion. These systems are listed and defined below and typically include:

- records management — aids in the management of records (paper and electronic), including the use of a file plan for classifying records and retention scheduling for identifying records due for disposition;

- document management — automates the preparation, organization, tracking, and distribution of electronic documents;

- storage management for both electronic and non-lectronic information — creates and maintains a centralized backup and recovery software system;

- facilities management — maintains a database of information about an organization's maintenance operations; and

- information systems management — creates and maintains an organized set of procedures and techniques designed to store, retrieve, manipulate, analyze, and display information.[7]

There may be additional system functionality needed for your organization, depending on characteristics such as size, type of industry, and the number of countries in which the organization conducts business.

Mapping the Flow of Information

Mapping the flow of information can be extremely helpful in mitigating risk. Knowing who has the authorization to do what with each item of information can and will greatly reduce the relevant risks. This assumes, of course, that appropriate security measures have been put into place to ensure that clearance for sensitive information is limited to those with appropriate access rights. Systematic audits of these security measures are needed to help guarantee conformity. Lack of attention to these elements can have catastrophic results, including organizational failure.

Retention and Disposition of Information

The final step is the disposition phase. The proper retention and disposition of information has never been more important — or more difficult. Of course, it's not enough to simply have a policy regarding the retention and disposition of information. The policy must be followed — consistently. And it must be in line with best practices and relevant regulations.

Retention requirements should be determined when the information is created or received by the organization. This is one of the most important elements of the record's profile. Discussed earlier was the meaning of the term "compliance" and the effect it has on how a company's policy for records retention should be determined. However, transitioning from the use phase to the retention phase is not as simple as it may sound.

In years past, when the preponderance of records were kept in paper form, organizations simply gathered together the documents that were no longer needed on a daily basis, placed them into a box, and moved them into a warehouse or storage facility. Unfortunately, far too many organizations continue this antiquated practice — focusing only on the paper component of the company's records and, by doing so, exposing themselves to unnecessary risks. The risks of retaining or destroying these records (irrespective of the records' format or media) have always been present, in the form of regulatory sanctions or court-imposed fines. Too often, though, organizations ignore the media-independent nature of records and retain electronic records differently. This introduces unnecessary risk with respect to legal challenges in electronic discovery and increased organizational costs in electronic or physical storage.

Electronic Discovery

An organization that disposes of information improperly may also be in danger of a lawsuit or regulatory sanctions. An organization that

holds onto information longer than necessary may be exposed to unnecessary costs associated with having to comply with electronic discovery demands that will require that they sift through a much greater volume of information than necessary.

To avoid these pitfalls, an organization should take certain steps.

- Ensure that during the creation phase, a profile is created that includes the determination of a retention period.

- Require regular reporting using a combination of electronic records, document, and e-mail management systems to provide sufficient notice of the information that has become inactive and is no longer essential to the everyday function of the organization.

- Document the retention process well to foster internal compliance, to ensure the organization's compliance with legal requirements and government regulations, and to safeguard the wellbeing of the organization. Make no mistake: The organization's reputation can be at risk as it publicly defends itself — in a court of law or through the court of public opinion — against challenges of its records management policies.

- As information reaches the end of its retention period, destroy it in a way that protects the organizations and customers from the risk of theft or data being called into question in court.

Enterprisewide Training

A solid, up-to-date RIM policy is just one piece of the puzzle, of course. The piece most often missing is enterprisewide training. Information is created and received at the desktop, so that's where the management process must begin.

"Organizations work through individuals," states the Hon. Ronald J. Hedges, U.S. Magistrate Judge for the U.S. District Court for the District of New Jersey. "So, up and down the reporting chain of an organization — whether that organization is a public or private one — the individual employee has a central responsibility for the management of the information, the retention of the information, or the production of the information."[8]

The message that managing records and information is a priority strategy for the organization and is everyone's responsibility must come from the top — beginning at the board level. The executive level must reinforce the message by providing adequate resources to execute the strategy and demonstrate its importance by management's work patterns and use of the systems.

Implementation of an enterprisewide training program must start by helping staff to understand just how important records and information management is to the organization and the role all employees play as

they strategically and efficiently manage the information of the organization. This should be regarded as basic staff training.[9]

Planning for Business Continuity

Being prepared for disasters is an important element of risk management. Disasters can be big or small, acts of God or manmade. Regardless, getting operations back up and running as soon as possible is imperative to the continued existence of an organization. *ComputerWeekly.com* recently reported that, according to a study by the University of Texas, 94 percent of companies suffering a catastrophic data loss will not survive.[10]

It's only logical, then, that most organizations would have a business continuity plan in place. Right? Wrong! The 2006 Business Continuity Market Survey conducted by OpenSky Research found that nearly 50 percent of businesses do not have a business continuity plan. Furthermore, almost 13 percent reportedly have no plans to implement one.[11]

A business continuity plan is a fundamental part of any RIM program. It outlines the necessary steps to protect companies from any unplanned interruption that prevents normal access to business-critical records and information technology (IT) applications. It should represent an organization's systematic strategy to protect business-critical information and to respond to any type of disaster that may have an impact on its facilities. Without such a plan, the business' critical records are left in a void, inaccessible to the business as it tries to return to normal business operations. This critical information could include receivables, payroll information, sensitive customer information, or other vital records that are crucial to the survival of the business.

Regardless of whether an organization has a formal RIM program, it must have a business continuity plan. At the very least, it needs to identify the records and information that are critical to getting the business operational following an emergency. Responsibility for maintaining and protecting those records should be clearly assigned, preferably to a professional trained in the management of records and information.

The business continuity plan should be well thought out and consider both likely and unlikely threats to business continuity. Backing up records and information from an IT perspective is a routine order of business. A copy of those backups, however, must be then stored off-site in the event of a localized disaster that shuts down access to the entire facility. The secure off-site facility should be protected from likely disasters that could occur in both locations simultaneously. Storage alone is just one element of the plan. A quality business continuity plan also includes tactics for contacting all employees for a return to operations, an alternate work location, and access to business equipment that will allow operations to restart.

Assessing the Risk

Analysis and assessment of risks to information are critical to producing a cost-effective business continuity plan. Risk assessment identifies the probability that records and information, and other valuable assets, will be damaged or lost. Risk analysis examines *existing* risk to records and information and *possible* loss exposures resulting from hazards, changing conditions, and system failures.

How do you determine if your enterprise's records and information management program — which comprises policies, procedures, and technology — presents a potential liability? Unfortunately, if you ask, IT may say one thing, records management another, and the legal staff yet another. That's because each answers from a different perspective, and each perspective is critical to determining the enterprise's status. No one department holds all the answers you need to determine the level of risk.

Risk management, legal, IT, and RIM must all work together to ensure the organization is well-protected. A good starting place is a self-assessment. Whether you build your own or use online self-assessments,[12] the assessment tool should require input from the key players — specifically, IT, RIM, and legal — to ensure an accurate analysis. Just as importantly, the tool should be based on current standards, best practices, and case law.

ISO Standard 15489

There are a variety of applicable national and international standards that address various elements of managing records and information. The fundamental standard is ISO 15489, the international records management standard. This two-part standard provides guidance on managing records to ensure they are created, captured, and managed appropriately — regardless of format and media. It specifies the elements of records management and defines the necessary results or outcomes to be achieved. It also provides guidance on supporting a quality process framework to comply with ISO 9001 and ISO 14001.

Part 2 of the standard is a supplementary technical report to the general standard. It provides further explanation and a methodology for implementation of the standard. This part specifically addresses

- policies and responsibilities;
- strategies, design, and implementation;
- processes and controls;
- monitoring and auditing; and
- training.

Other American National Standards

In addition to ISO 15489, there are several American national standards that address various elements of records and information management. These include:

- *Requirements for Managing Electronic Messages as Records (ANSI/ARMA 9-2004)*, which defines the necessary elements of a corporate policy

for managing information content in any type of text-based electronic message;

- *Retention Management for Records and Information (ANSI/ARMA 8-2005)*, which provides guidance for establishing and operating a retention and disposition program; and

- *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records (ANSI/ARMA 5-2003)*, which sets the requirements for establishing a vital records program.

Online Assessment Tools

Online self-assessment tools are based on these standards as well as recent case law and current best practices. Some tools focus specifically on records management. They ask questions about:

- policies and procedures;

- program structure;

- classification plan effectiveness;

- records security and protection;

- active program effectiveness (i.e., the handling of an invoice before it is paid — these are records that are subject to frequent use and usually located near the user);

- inactive program effectiveness (i.e., the treatment of an invoice after it is paid and before it is destroyed or archived); and

- monitoring and training.

Interestingly, some major insurance companies are using questions based on such tools as part of their risk assessment process.

Another kind of tool goes a step further and provides a diagnostic analysis of the organization’s e-discovery readiness. Such a tool looks at a variety of areas including:

- policies and responsibilities;
- strategies, design, and implementation;
- records process and controls;
- monitoring and auditing;
- training;
- litigation holds;
- evidence collection and preservation;
- electronic data production planning; and
- processes for producing electronic data.

Litigation holds — which call for the immediate suspension of the destruction of records that otherwise could be destroyed according to the organization's retention policy — deserve additional discussion. As litigation and electronic discovery become the normal course of business for organizations, a litigation holds policy is needed to safeguard potential evidence. The policy acts as a directive to employees, providing directions for the safe handling and preservation of information that may be called into court during a trial. A litigation hold may call for the preservation of, for example, all files related to a given topic or simply the entire contents of one employee's computer and paper files.

Finally, cyber-security self-assessment tools evaluate the organization's computer network resources and information assets.

Once you've identified the areas where there is highest vulnerability, steps can be taken to address the problems. Again, all relevant parties — legal, IT, and records management — should be part of the strategizing and implementing for solutions to be successful.

Avoiding Pitfalls

There are no shortcuts when it comes to minimizing information management risks. Despite what some vendors state in their advertisements, simply implementing a software package isn't going to do the job for you. For example, there is no such thing "Sarbanes-Oxley-compliant" software. There are applications that can facilitate compliance, but for them to be effective, the prerequisite policies and procedures must be in place. Further, the policies and procedures should drive the software design.

Given the complex nature of information management risk, corporations find need for collaboration among those who are setting the policies and procedures and those who are implementing the systems. Policies independent from procedures can lead to ineffective systems, wasted resources, and higher risk.

Similarly, policies, procedures, and systems aren't effective if the entire enterprise is not aware of them and implementing them daily. The importance of enterprisewide training cannot be stressed enough. Just as with a business continuity plan, the program is worthless if no one knows what it is or if it's out of date.

Endnotes

1. INDICTMENT: Cr. No. (T. 18, U.S.C., §§ 1512(b)(2) and 3551 et seq.) Available online a: http://news.findlaw.com/hdocs/docs/enron/usandersen030702ind.html.
2. ARMA International, "Recent Rulings Refocus Attention on Records Retention." Available online at *www.arma.org/news/index.cfm?NewsID=320&Type=Industry*.
3. *United States v. Philip Morris, USA, Inc.,* No. CIV.A.99-2496, 2004 WL 1627252 (D.D.C. July 21 2004).

4. ARMA International, *Glossary of Records and Information Management Terms* (ANSI/ARMA 10-1999). (ARMA International: Prairie Village, KS, 2000).
5. "Old Mutual Client Data Are Stolen," *The Wall Street Journal* (July 25, 2006): C13.
6. All of these bills can be found at http://www.govtrack.us/congress/bill.xpd.
7. Arma International, *Glossary*, ibid.
8. Kahn Consulting Inc. and ARMA International, *Keeping Good Company: How Information Management Drives Accountability, Competitiveness, and Compliance* DVD training program (2005). Available at www.arma.org/learningcenter/goodcompany.
9. As of this writing, there is only one training program available, "Keeping Good Company: How Information Management Drives Accountability, Competitiveness, and Compliance," id.
10. Beckett, Helen, "SMB Focus: Make sure it is business as usual," *Computer-Weekly.com* (March 7, 2006). Available at http://www.computerweekly.com/Articles/2006/03/07/214522/SMBFocusMakesureitisbusinessasusual.htm.
11. "Nearly 50 Percent of Businesses Lack Continuity Plan, New Survey Shows," OpenSky Research (March 2006). Available at http://www.neverfailgroup.com/news/press/2006/q1/march/21.aspx.
12. Online assessments are available through ARMA International at www.arma.org/profiler, as well as from other sources.

William Millican is the Director of Professional Resources and Standards for ARMA International. He has more than 20 years' experience as a records information management consultant and practitioner. He may be reached at wmillican@arma.org.

About ARMA

ARMA is a not-for-profit professional association and authority on managing records and information. ARMA International offers education, standards, and other resources on myriad topics related to the management of records and information as corporate assets. For more information, see www.arma.org.