

Document Management and Retention-Why?

The issues behind a document strategy

Written by David Waterson, IKON Office Solutions

Presented 10/20/2005 to the Air Capital Chapter of the
Association of Information Technology Professionals,
Wichita, KS

TABLE OF CONTENTS

Introduction3

Regulatory Compliance.....3

Business Continuity Planning.....5

Cost Factors.....7

Conclusion/Contact Information.....9

Introduction

The purpose of this white paper is to address current issues surrounding Document Management and Retention; and the influences both external and internal that organizations are facing today regarding creating and managing a document strategy.

There is a compelling issue behind the topic. Numerous independent research groups such as Gartner, IDC, and CapVentures have performed studies and discovered that the average company spends between 5 and 15 percent of its corporate revenues on the creation, distribution, storage and retrieval of its office documents. A simple exercise to help understand the impact those activities have on your organization is to write down your company's annual revenue number and move the decimal point one digit to the left. The resulting number will give you a general idea of what office documents mean to the bottom line of your organization. The goal for most companies is to make that number smaller. Or preferably, redirect a portion of it to activities that make the annual revenue number bigger.

Against that goal, the world of IT is changing. IT is being asked to move from the server room to the boardroom, to help make strategic decisions regarding business critical information. Now more than ever IT is being asked to provide organizations with a competitive advantage; protection from evil-doers; cost reductions; business plans...the IT world changing both internally and externally, and at times it may be difficult to bear.

Business today finds itself pressured to make changes. Often times outside influences prompt a shift in the way that documents are created, distributed, archived, and retrieved inside an organization. These influences can cause an implementation of technology without really understanding current costs and risk factors, as well as some important business and technical issues. This white paper addresses three influences driving the need for a document strategy: Regulatory Compliance, Business Continuity Planning, and Cost Factors.

Regulatory Compliance

One influence driving the need for a document strategy is regulatory compliance. Regulations such as SOX, HIPAA, GLBA, etc are doing two things: first, it is causing stress to anybody whose job title begins with the letter C. Second, the number of different compliance standards is causing great confusion for businesses. The acts are very complex in scope and intentionally ambiguous...they do not provide clear guidance on the procedures that organizations have to follow in order to stay compliant. In addition, the rules keep changing as technology becomes available. Organizations need to understand the requirements of the acts and decide on protocols and controls that need to be implemented in order to stay compliant.

Publicly traded companies are subject to the rules and regulations of Sarbanes-Oxley. The Sarbanes-Oxley Act, or SOX, was passed in July 2002 as a result of public scandals regarding dishonest financial reporting. SOX requires all publicly traded organizations to implement appropriate controls for financial reporting. Specifically, SOX requires that companies manage their internal controls and ensure financial governance and accountability. Although the act is very broad in scope and encompasses 11 titles, Kansas citizens have seen firsthand why the SOX exists. On September 12th, 2005, David Wittig and Douglas Lake were convicted on a combined 69 counts of fraud,

conspiracy, and money laundering from their corrupt tenures at Westar Energies. The main goal behind Sarbanes-Oxley is to discourage such activity from occurring in other publicly traded organizations across the country.

Perhaps the most infamous regulatory act in the document management space is the HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, or HIPAA. HIPAA was passed by legislation in 1996 in order to protect the privacy of patient records, and any organization that handles personal health information in any form is subject to HIPAA regulations. HIPAA's reach expanded beyond the traditional hospital and clinic in 2003 with the introduction of a Privacy Rule that requires all organizations handling patient health information to have the appropriate administrative, technical and physical controls in place to ensure that patient information is secure and kept private. Because of the Privacy Rule, HIPAA now regulates attorneys, insurance providers, and any other entity that processes confidential health information.

Some examples of the organizations besides clinics and hospitals that are affected by HIPAA are:

- Health plan providers and related claims processing entities
- Health care clearinghouses including billing services, repricing companies, and community health management information systems, all of which are required to ensure that patient data is transmitted confidentially.
- Any other business that performs the functions of data analysis, utilization review and billing, or legal representation.

HIPAA is an entity that is funded primarily by the fines that it levies. Failure to satisfy the HIPAA compliances could cost a practice as much as \$100,000 per infraction.

There are a few simple questions you can ask yourself regarding whether or not a process is HIPAA compliant. Those questions are, "what would it take for this information to fall into the wrong hands?", and "How do I find out whose hands it fell into?"

What HIPAA is to medical information, the Gramm-Leach-Bliley act is to financial information. The Gramm-Leach-Bliley act, passed by congress in 1999 and enforced by the FTC, requires all financial institutions and organizations working with their customer's private financial information to establish control and security policies for protecting that information.

GLBA consists of two basic parts; the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule controls the collection and disclosure of private financial information, while the Safeguards Rule requires that financial institutions establish controls and safeguards to ensure that customer information is kept private.

GLBA applies primarily to banks, securities firms and insurance companies. But like HIPAA, GLBA can also apply to companies that work in conjunction with financial products or services such as:

- Loan and Mortgage brokers
- Accountants
- Debt collectors
- Financial advisors

The fine structure for Gramm-Leach is also very similar to that of HIPAA. For instance, if a financial institution is found to be in violation, the financial institution shall be subject to a civil penalty of not more than \$100,000 for each violation; AND the officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than \$10,000 for each violation

And if that isn't enough, the officers and directors can go to prison for up to five years. That is why one of the taglines of this conversation is ROI: Return on Investment, Risk of Incarceration, or both!

Chances are if your company is directly affected by any of these regulations, you've already taken the steps necessary to become compliant. However, the rules are liable to change as technology changes, and maybe even more importantly, technology is still changing to make compliance more cost-effective. Again alluding to the 5-15% of corporate revenues that are wrapped up in office documents, a compliancy strategy that was developed two years ago may be costing your organization more than it needs to today.

For instance, most Healthcare providers have complied with HIPAA by implementing an electronic medical records system with the capability to monitor "who" is viewing documents, and also makes the process of finding information quick and easy. Today, the area of focus for cost reduction is shifting more towards the input and distribution processes of those records. The good news is that there is now technology that streamlines the document distribution process and also meets the needs for monitoring who is seeing what information when. A downside to the number of technology solutions available today is that there are many software companies that claim to have "compliance software", and such a thing **does not exist**. Compliance requires education and strategy, not software...so buyers beware of software marketed as a compliance solution!

An organization that isn't subject to some sort of regulation should still have some of the same strategies in place. The basics are: archive your documents for at least seven years in a manner that allows for easy retrieval if an audit is necessary and put safeguards in place to make sure the information in those documents remains secure. If it is not possible to monitor who is looking at documents, when, and why, then chances are that the organization is left vulnerable. Also think of emails, instant messages, etc, as those are also documents and just as important to monitor. The general rule is to keep anything that has a signature or financial information...it obviously isn't necessary to keep an inter-office memo inviting all staff to the Christmas office party. The best thing to do is to work with your main process owners to determine what is critical business information and what is not, and then develop a document strategy around the critical documents.

Business Continuity Planning

Business continuity planning and disaster recovery have been conversation topics for a while now, but the unusually active Hurricane season has shed some recent heat and light on the topic. The following are three examples of very different experiences regarding disaster recovery and Hurricane Katrina.

"I am friends with the wife of an Operations VP for a national company. This company, who shall remain anonymous, is a franchise of sorts with locations in most major cities across America. This company had a location in New Orleans, and that particular location had opted to store all of its files in paper form in file cabinets.

Two weeks ago, my colleague described a home movie she had seen over the weekend. The video was shot by her husband, who had journeyed to New Orleans with other operations officers to survey the damage inflicted to their New Orleans location by Katrina. The video opened with a walk-around of the facility, in which the force of raging floodwaters could be seen etched four feet high in the walls of the buildings.

Inside the business office, everything was covered with mud. Literally. It looked like brown snowdrifts piled over desks, computers, file cabinets, etc. At one point the operations officers opened a file cabinet to examine the records inside. As you could probably imagine, the paper was totally destroyed. In the audio background you can hear a dejected voice mutter, 'well, we're done here.' Decades of business had disappeared in a matter of hours. "

You can contrast that experience with one reported recently by CNN. In the wake of the Katrina catastrophe, crucial medical services were in danger of being denied to those who need them most. One bright exception is that even though the New Orleans VA Medical Center flooded, electronic medical records for 50,000 patients of that hospital and surrounding veterans' outpatient clinics survived. The following is an excerpt from that CNN article:

"On September 1, three days after Katrina hit the Gulf Coast, a Veterans Affairs Department computer specialist was airlifted from New Orleans carrying backup tapes of all the records, which by the next night had been re-entered into computers in Houston.

"Every single thing on that computer was saved," said Charlie Gephart, records chief for the South-Central Healthcare Network.

Moreover, evacuees could access some records even at the height of the disaster, Gephart said. His office put patient prescriptions and other data tracked at a separate location onto a secure Web site as an interim solution.

Health and Human Services Secretary Mike Leavitt described the state of affairs to The Associated Press on Monday "There may not have been an experience that demonstrates, for me or the country, more powerfully the need for electronic health records than Katrina," "This is not going to be a short-term problem."

If anybody was prepared for a disaster like Katrina it was the medical community due to the large amount of publicity and interest that Electronic Medical Records has received over the last few years. This is in no small part thanks to the aforementioned HIPAA. Unfortunately, not every industry has been as pro-active in guarding customer information from flood, tornado, fire, earthquake, etc.

“A few years ago I arrived at an appointment with a sales rep at a manufacturing firm in Abilene. We walked in through the front door and asked for the gentleman that we were there to see. He walked in and shook our hands and told us that he didn’t have much time because something had come up. He went on to tell us that a fire had occurred the night before. We were there to talk about replacing a copier, and he walked us back to where the machine used to be. Although the entry appeared normal, as we made it further down the corridor the walls and ceiling grew progressively darker with soot. We finally made it to a back room, which he told us was where the banker boxes of customer and product information had been stored. Everything was gone. We found out later that a disgruntled former employee intentionally set the fire. I found it interesting that the file room was the former employee’s target, as he was determined to put the business out of business.”

You don’t need a disgruntled employee to have a disaster. Disasters come in many forms, and it is easy to focus on the catastrophes such as a fire or flood, but there are little disasters that happen every day. If a file is misplaced, lost, or accidentally destroyed, isn’t that a little disaster? What is the recovery plan for the little disasters?

Cost Factors

When weighing the cost against the benefit of a “disaster recovery system”, there are a few different cost centers. The first would be accounts receivable. Most businesses trade product for money, and in many cases the product goes out before the money comes in. If an order is written and the record of that order is paper-based or never leaves site, it is vulnerable to becoming victim of a disaster. How much money is currently in your organization’s accounts receivable system? What happens if you no longer have record of those transactions? Will you ever collect?

In the case of manufacturers, many documents have to be on file in case the products that are manufactured ever cause a lawsuit. In Wichita, The Air Capitol of the World, numerous manufacturers have to keep schematics, certifications, part histories, and other related documents forever just to protect themselves should a plane ever fall from the sky. If such an event should happen, how does a business find the information that is needed to defend itself in a timely manner? What happens if the information can’t be found?

Another way of looking at it is the value of one customer to your business. Imagine what it would be like if your organization had a disaster and lost valuable customer information because of it. How many of your customers would continue to do business with you? How many would put up with the frustration of not getting the level of customer service they are used to, simply because the necessary data isn’t available? If 10% of your customers went elsewhere seeking better customer service, what would that mean to your company’s bottom-line?

Although this form of disaster recovery is a compelling topic, there is interesting data behind some other arguments for a document strategy. If implemented appropriately, a document strategy can actually add dollars back to the annual revenue number.

There was a 2001 Coopers and Lybrand study that found that the average paper-based office document costs \$20 to file, \$20 to retrieve, \$120 to locate if it has been mis-filed, and \$250 to re-create if lost. In the modern office environment, those numbers can add up in a hurry, and go largely un-audited due to the nature of the work. Think of it this way: in a manufacturing environment, operations specialists spend countless hours and dollars quantifying the cost to produce one “widget”. They can tell you down to the sixth decimal point what it costs to produce that product. However, there are few people in the office environment can tell you with any accuracy at all what it costs to produce, move, and inventory a document.

The numbers are staggering. On average, a financial institution that has 100 employees and annual revenue of \$10,000,000 per year will spend \$456,000 on paper-based document storage and retrieval. If a strategy was implemented that decreased that annual spend by a measly 20%, it would add \$91,000 a year back to the bottom line. And the scary part? The total document-related spend for that bank...creation, distribution, storage, and retrieval...comes in at almost a million dollars annually.

Most offices today are aware of the hard printing costs and are beginning to manage the activities surrounding them, but overlook the activities surround document management. Here's a quick tidbit for you: For every dollar that an organization spends printing an office document, there is 7 dollars spent moving and storing that document. And the costs just get duplicated as more copies are made.

A great story that illustrates the process around the paper: Imagine for a moment an organization that has enjoyed the same customer base for years upon years. Imagine the customer service process that was in place a few years ago: The customer calls in with a dispute...maybe claiming that a delivery wasn't made and questioning the validity of the corresponding invoice. Customer Service answers that call on nearly an hourly basis.

What most people don't see is the process after that phone call is over. The CSR who answered the call now has to go to the file cabinet, find the order, dig out the page with the signature, track down the fax number, fax the order to the customer, make a note that the call was received and the order has been faxed, call the customer back to make sure the fax was received, and if it wasn't... repeat the process. Depending on how well the files are kept in order and how cooperative the customer wants to be, this could take HOURS.

Imagine now the same scenario. The customer calls in, hot under the collar. The customer service rep asks for an invoice number, and keys it into the computer. An image of the invoice appears on the screen, complete with corresponding order packet. The CSR asks the customer for their email address, and emails the signed order and

delivery acceptance certificate without ever hanging up the phone. The process that used to take hours now takes minutes.

What does that do to the bottom line of the company? For starters, you no longer need as many CSRs. If your customer service staff goes from four employees answering calls and resolving issues to two employees, one scanning and indexing and the other resolving issues, what does that add back to the bottom line in terms of hard salary alone?

And what about the customer experience? What does that do to customer retention if the people giving you money now know that they can call with an issue and expect resolution before they are off the phone? One of the first things that anybody with a marketing degree will tell you is that it is 10 times more costly to win a new customer than it is to maintain a customer you already have.

The average business has access to about 16% of its collective knowledge. Data is an easy thing to share, but paper is not. How do two salespeople sitting on opposite sides of the country see the business knowledge that exists in paper form in the file cabinet at headquarters? How do we share that? Make a copy and mail it? 37 cents for the stamp, 2 cents for the copy, and three days for the pleasure of snail mail. Do we fax it? That's even more expensive. We can scan it and email it, but what happens if two weeks later somebody else needs to see it, and then a week later it happens again? Is it cost effective to continually scan and email a piece of paper? That is a major reason why imaging exists, so that a business can share information out to those who need it to get their job done.

Conclusion

So whether the goal is to comply with government regulations, guard your business against the effects of a disaster, or use technology to positively affect productivity and the bottom line, there are numerous reasons why imaging makes sense for your business. Although the "paperless office" concept may never truly exist in the modern office environment, a good document strategy can reap rewards in many areas for your organization. I encourage every reader of this document to start the conversation within his or her organization, to address the issues that make document management and retention a topic in business today.

If you have questions or feedback and would like to reach the author of this whitepaper, email dwateron@ikon.com.