

E-mail maelstrom

Electronic documents must be managed.

By Ronald Raether

Records! First it was paper, but now electronic documents clog the office systems of our clients — and ourselves. What's the best way to deal with them?

Businesses traditionally have recognized the benefits of good planning and practices for managing paper documents. With document retention policies, dedicated space and whole departments responsible for tracking and managing documents, the need justified the expense.

Even in the dawn of time in the '60s, the problem was obvious. As one article noted: "The need for paperwork is justified but the economic waste resulting from the inefficient handling of paperwork is not justified. [R]ecords waste constitutes a serious reduction from the organization's annual profits" Mary Claire Griffin, "Records Management: A Modern Tool for Business." (1964)

The medium has changed, but the need is the same for electronic information. A recent University of California, Berkeley, study found that 99.997 percent of all documents are created and stored electronically, that office workers exchanged an estimated 2.8 billion e-mails a day and that by 2005, corporations will generate more than 17.5 trillion electronic documents annually. Peter Lyman & Hal Varian, "How Much Information?" (2000) at <http://info.berkeley.edu/how-much-info>.

Yet most businesses have not taken the steps necessary to be sure that outdated (and often abandoned) docu-

ment management practices can deal with electronic information. Other businesses have attempted to address electronic information but missed critical elements in having an effective policy. As novelist James Agee once said, "You must be in tune with the times and prepared to break with tradition." Failure to change can be disastrous; the benefits are tangible.

We have all heard about cases where electronic documents played a key role in the outcome. The Enron obstruction of justice trial of Arthur Andersen provides a good example. In finding the accounting firm guilty, the jury focused on one e-mail from an in-house lawyer at Arthur Andersen to the Andersen partner responsible for the Enron client relationship that, among other things, suggested deleting some language "that might suggest we have concluded the release is misleading." Tom Fowler, "Lawyers fear legal impact of Andersen: They ask if advice might be a crime," *Houston Chronicle*, June 25, 2002, at <http://www.chron.com/cs/CDA/story.hts/business/1468838>. The e-mail turned out to be pivotal in the jury deliberations to convict Arthur Andersen.

While sound policies may not avoid the creation of such damaging documents, educating employees on the proper use of e-mail and other electronic documents can help. Surprisingly, only 34 percent of employers had written e-mail retention and deletion policies in place as of April, 2001. American Management Association, *U.S. News & World Report* and The ePolicy Institute, "2003 Electronic Policies and Practices Survey," at <http://www.epolicyinstitute.com/survey>.

As five major firms recently learned after being fined a total of \$8.25 million for not preserving e-mail messages, the absence of sound policies can be costly. Tim Paradis, "Message to Wall Street: Save Your E-mail," *Wall Street Journal*, Dec. 4, 2002.

Today, many companies have adopted such e-mail and other electronic document policies. But even for those firms that have electronic document policies, such policies often fail to account for many concerns unique to dealing with electronic information.

While this article does not provide an exhaustive road map to guide every business, it does identify a number of issues and broad categories often overlooked when developing an electronic document policy. In the end, understanding the points outlined in this article will help to create sound electronic document management policies, which will improve the efficiency of the organization and better prepare the company for litigation.

So what can be done?

Of course, the place to start is with the existing electronic document policies, if any exist. This article discusses three broad areas important in evaluating existing policies or to create new policies to ensure effective electronic document management:

- knowledge management (that is, when and how),
- system knowledge (that is, what and where), and
- accountability (that is, who).

The first step in effective electronic document management is to have sound company policies. But what should the policies cover? First, any policy should regulate the use of e-mails, providing clear guidelines for

Raether is a senior associate at Faruki Ireland & Cox P.L.L., in Dayton, Ohio. His e-mail is rRaether@ficlaw.com.

when and how to use e-mail.

Likewise, the policy should state clearly how and when company information may be transmitted electronically, and identify what information should be retained and where it will be kept in the system. With the ease of moving large amounts of information electronically, these policies are important to protecting the trade secret status of proprietary information and enhancing the ability to locate the information later and improve efficiencies.

But the scope of any policy should not be limited to just the general use of e-mails and transmitting electronic information. Companies also should have clear policies concerning the treatment of electronic information in the possession of terminated employees. These policies become especially critical for telecommuting employees.

For terminated employees, it is important to have clear policies on the return of electronic information, phone lines and equipment or other sources that may contain electronic information such as PDAs (personal document assistants) and cell phones. Included in this policy should be a clear directive as to where this information should be returned. The policy also should include checking the hard drive and other electronic equipment for employees that handle sensitive company information, especially e-mail files. Internal controls related to these policies are critical. Otherwise, important company information could be lost once the hard drive is erased for the next user.

Fortunately for one of my clients, such a policy existed. A former employee e-mailed confidential information to her personal address the day before she suddenly stopped coming to work. Her supervisor reviewed her e-mail accounts and discovered that confidential information had been taken.

The client had an e-mail policy that provided:

Forwarding electronic mail to an external network address: Unless the

information owner/originator agrees or the information is clearly public in nature, associates must not forward electronic mail to any address outside the company's network. Automatic redirection of electronic messages to any outside address is prohibited.

In part, because of this policy, a court issued a temporary restraining order and the information was returned. Without these policies, my

.....

Here comes that claim of spoliation.

.....

client may never had learned that the information had been passed outside the company, let alone secured its return.

This same result was achieved in *Equus Computer Sys. Inc. v. Northern Computer Sys. Inc.*, No. 01-657 (DWF/AJB), 2002 U.S. Dist. LEXIS 13539, at *11-12 (D. Minn. July 22, 2002), where the existence of an e-mail policy prohibiting the disclosure of trade secrets or confidential information, together with the limited distribution of the customer information at issue, led the court to uphold the temporary restraining order since there was a significant likelihood that the information was protectable. For companies in highly competitive markets, such policies could make a significant difference.

An area also often overlooked in company policies is customer data and related electronic information. For a company storing critical customer data electronically (almost everyone today), leasing hardware or acting as an application service provider, these policies are important to avoid liability for violating statutes (such as, HIPPA, 42 U.S.C. §§ 1320d-1320d-8), confidentiality/nondisclosure agreements, or privacy policies.

If customer data is still on returned equipment, then protocols are needed for how this information is to be handled. These policies can be equally crucial for companies that sell or donate their old computers. Instances of purchasers of used or refurbished computers discovering personal information that the previous owner had left on the computer are not as rare as they should be.

For example, a hospital in Indianapolis sold its old computers to a thrift store. With the help of a computer forensics expert, the local news station retrieved not only patient records, but the hospital's privacy policy stating that the computer hard drives should be completely erased before being sold.

Another important issue sometimes overlooked (especially concerning e-mails) is how long an electronic file should be kept. Whatever the answer, you should be certain that a reasonable business justification exists for the time period selected. Regardless, your plan must include ways to stop the destruction of electronic files should litigation arise. Otherwise, the company could be subject to a claim of spoliation.

Such policies must be effective, complete and comply with existing law. The failure to do so can be costly. For example, in *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598 (D.N.J. 1997), the defendant was ordered to preserve all documents relevant to the litigation. Prudential communicated by e-mail to its sales force the need to preserve brochures and other material for litigation. Unfor-

tunately, documents were nonetheless destroyed by some of the sales force who never read their e-mail. The court imposed a \$1 million fine as a sanction.

Sanctions also have been imposed when a party produced the requested electronic documents, but then destroyed the original electronic versions of the documents following its normal document deletion policy. *Applied Telematics v. Sprint Communs. Co., L.P.*, No. 94-4603, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa. Sept. 17, 1996).

For companies without sound policies, an order to preserve documents can present an insurmountable hurdle. If the electronic files are not organized properly, then how can the company be certain that the destruction of certain electronic files will not destroy relevant evidence? Often, the only answer is to keep all electronic files or to require employees to keep a log of all destroyed documents — obviously costly and possibly disruptive requirements for some companies. The more cost-effective solution is to implement sound policies and enforce them.

For larger organizations, another problem is learning what individuals in the organization have relevant documents. With the prolific use of e-mails, the ease of sending copies to an unlimited number of people, and the overuse of string e-mails, this problem can be enormous. Policies setting standards as to e-mail use such as requiring employees to generate new e-mails rather than forwarding unrelated e-mails (a.k.a. string e-mails) can curb this problem.

But sound policies are only the beginning.

Other benefits only can be achieved by knowing your systems, managing your knowledge, and ensuring accountability — factors often overlooked in many company policies. System knowledge requires an understanding of the overall system network, that is, who has the information, where the information is located, and what kind of information exists? Simply telling people to save information is not enough. However, the answers to these questions will vary depending on the size and

complexity of the organization.

The types of electronic information generated by a company often include correspondence, accounting information, contracts, e-mails, customer service notes, presentations, business plans — the list goes on and on. The content can range from office gossip to mission-critical documents. The key is understanding what type of information is being generated and by whom.

Without understanding your clients' systems and business, it is impossible to have an effective electronic document retention policy. Companies should

device and on how it is used.

Fed. R. Civ. P. 34 requires respondents to produce all relevant documents (and data) that are in "the possession, custody or control of the party upon whom the document request is served." Rule 34 also has been applied to discoverable items in the possession of former employees, to the extent a company had any control over them. *In re Folding Carton Antitrust Litig.*, 76 F.R.D. 420, 423 (D.Ill. 1977).

Policies often overlook many sources of electronic information, such as Web sites, electronic bulletin boards, virtual collaborative tools (such as, electronic mark & wipe boards), and even voice mail. In *Kleiner v. Burns*, No. 00-2160-JWL, 2000 U.S. Dist. LEXIS 21850, at *11-12 (D. Kan. Dec. 22, 2000), the court held that:

computerized data and other electronically recorded information includes, but is not limited to: voice mail messages and files, back-up voice mail files, e-mail messages and files, back-up e-mail files, deleted e-mails, data files, program files, back-up and archival tapes, temporary files, system history files, Web site information stored in textual, graphical or audio format, Web site log files, cache files, cookies, and other electronically recorded information.

With expanded functionality, even an employee's cell phone is likely to have discoverable information (or trade secrets), such as e-mails, a phone list or "to do" notes.

As mentioned previously, company policies must not only address the above source variations, but also matters of timing, and how and where the information is saved, such as back-ups and in what formats. A critical point occurs when a company changes technology. The old software and files become "legacy data." When responding to an information request, the problem is not only locating the data, but also knowing what software and hardware is needed to retrieve and read that data.

.....

Simply telling people to save information is not enough.

.....

keep a continuing inventory of their sources of electronic information, tracking by individual and projects the equipment being used. Your needs and requirements will differ depending on whether you operate in a network environment (servers/workstations), have virtual-office employees (or allow employees to work on their home personal computers), use PDAs, etc.

In fact, many companies overlook portable devices when drafting their policies. That could be a mistake. Information from these devices is discoverable regardless of who owns the device. Whether a company must produce information from portable devices in discovery depends not on who "owns" the device, but on "who controls" the

While many companies have policies regarding the retention of electronic documents, without knowing where the information is located and how to access it, it is virtually impossible to enforce these policies or to locate the information when needed.

With sound inventory plans, including retention of the legacy software and hardware, many problems can be averted. Companies should keep an inventory of their sources of electronic information, tracking by individual and projects the software and equipment that was used.

Moreover, proper knowledge management requires, among other things, sound methods that allow for the tracking of employee use and compliance with company procedures. Systems should be in place to ensure that electronic documents relating to a particular project or issue are indexed and can be located and separated from unrelated issues.

With the proper incentive, employees can learn the importance of complying with organizational procedures. Organization is important not only to obtain the business and litigation efficiencies discussed in this article, but also to avoid giving your adversary rights to explore files that contain trade secrets unrelated to the pending dispute.

To that end, there needs to be a single point of accountability.

Whether it is a single individual or group will vary depending on the size of the company and other matters. The more important factor is that your company has a single source to locate documents and if the process fails, then there is a single point to be held accountable. To check the sufficiency of the controls and procedures, the company should have tracking software. Employees also should receive periodic reminders, and the process should be audited occasionally.

Good policies, without enforcement, may not be enough. For example, Eli Lilly had a privacy policy in place. However, it nonetheless unintentionally disclosed the names of 669

Prozac users by openly putting their addresses in a bulk e-mail that the Prozac users had elected to receive. The incident became the first time the Federal Trade Commission prosecuted an unintentional violation of a Web site's privacy policy. Associated Press, "States settle with Lilly on e-mail," July 25, 2002. Eli Lilly settled the case for \$160,000.

Is it worth the expense and trouble of implementing such policies?

It certainly was for paper documents. The same benefits can be


• preserving company and legal resources to reduce expenses (including the "soft" expense of irritating business people with repeated and sometime intrusive requests), and

• allowing for the development of sound case strategies based on a review of all the important documents in the client's possession (that is, avoiding the surprise smoking gun).

These policies also avoid some of the unexpected pitfalls of electronic discovery. Electronic discovery can open your system to scrutiny in areas unrelated to the pending matter. For example, in *Playboy Enters. Inc. v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999), former Playmate Terri Welles was sued for trademark infringement for using the Playboy name and logo on her personal Web site. After she admitted deleting e-mails during litigation, the court ordered her to allow Playboy access to her hard drive to make a copy of it.

The implications are sobering. For example, in a dispute with a competitor, would you want their lawyers to have full access to your computer system, including matters not directly relevant to the pending dispute? If your electronic information is not indexed, then you may have to allow this intrusion.

Being prepared for electronic discovery provides tangible business-related benefits by allowing the company to better use and share valuable documents and data. Experiences and lessons can be shared; employees can better pass along valuable product or customer knowledge. With many communications by e-mail and many documents not being moved to paper, without a sound plan, much of this information is now lost.

With the proper incentive, employees can learn the importance of complying with organizational procedures needed not only to achieve these business and litigation efficiencies, but also to avoid serious consequences in the courtroom. Considering many of the issues raised in this article can help your client to develop policies that achieve these goals. 

.....

There must be a single point of accountability.

.....

achieved with electronic document policies. Recently created traps can be avoided. For example, the release of financial information without authorization to a nonaffiliate could violate the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6810 if it does not meet one of the exceptions. For health plans, clearinghouses or providers, the release of medical information without authorization could violate the Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d-1320d-8. Representations in public privacy policies also create risks.

In addition to avoiding these unnecessary risks, sound policies also can provide benefits in litigation by:

• reducing the time to locate and retrieve relevant documents,