

Article

The Liability of Email as Evidence

What You Don't Know May Hurt You

You can shred paper documents, but electronic files, including email, live on. And don't think that deleting them, or even emptying your recycle bin, is going to get rid of them. Out of sight may mean out of mind for most computer users, but the reality is most deleted files are still lurking on your computer, and everyone who uses email at work must understand the potential liabilities of email.

Contrary to popular opinion, "delete" doesn't mean erase permanently. When you delete an email, you're really just telling your computer that the space the email took up is now available to be overwritten. But with hard disks now being the size they are, few people ever use up all of their hard disk space, and consequently, their hard disks are only overwritten when they reformat their hard drive.

Even if the files are overwritten, fragments of the documents survive, sometimes in several places on a computer, because of the way most of us multitask with our computers. If, throughout the day, you switch back and forth between different applications—email, the Internet, Excel, and Word—each time you switch, whatever was on your monitor is saved as a temporary file in your RAM, and once the RAM is full, it will access your hard disk, which may then have fragments of your documents.

All software, including reformatting utilities and shredder programs, leaves signs that it has been used. The metadata and file properties provide such information as dates of creation and modification, number of revisions, and the identity of the person who worked on the document.

Electronic files leave trails on server logs and are backed up on servers, making them traceable and recoverable. Even when whole files are not recoverable, fragments survive, and the very fact that utilities and software have been used may be a red flag to investigators. Consider too that copies of electronic files and email messages may exist in a variety of locations in your company's computer system, as well as in the recipients' system and in the records of intermediaries within the transmission process.

What this means is that deleted electronic files can be recovered by forensics experts. And it isn't just the unscrupulous — those with something to hide — who need be concerned about what will come back to haunt them.

According to Lee Neubecker, President of Forensicon, a risk management and computer forensics company based in Chicago, "there are compelling reasons that a company that is operating ethically and within the bounds of the law needs to make sure it is permanently deleting documents. The risk of not controlling and managing information stored in electronic archives is huge."

Most companies, even those without document retention policies that force employees to save only official communication, have daily back up files on their servers, but it's naïve to think of these as a security blanket. They can be a liability, because if a company, pending litigation, is required to produce selected data, the time and expense it requires to have either in-house IT professionals or external consultants weed through those files are costly — more costly than proactively purging unnecessary files.

"For a company that doesn't have a document retention policy and has documents going back five years, having to produce electronic documents--as is quickly becoming commonplace in litigation--is extremely expensive," says Neubecker. "By instituting a document retention policy to eliminate unneeded documents on a regular basis, a company reduces its potential data universe, knows what is saved, saves money, and reduces its potential liability. The burden of not enforcing regular purging can be devastating."

When your data universe stored on back up files is vast, what you don't know may hurt you. Large corporations have a lot of people working for them, and it's virtually impossible to know the contents of what people send and receive. Never mind (if you dare) hackers and crackers and the upward trends in such cyber-crimes as sophisticated industrial espionage, trade secret and patent information theft, or even loose cannon employees who may be guilty of sexual harassment, leaking valuable company information, stealing databases with client information for a new position, or just jeopardizing company security by innocently copying files in order to work from home, think about the playful, off the cuff email comments with no serious intent that, taken out of context, may be misconstrued or scrutinized in litigation.

As Neubecker states, "What's important is that companies protect themselves from someone in the future inferring something that could be damaging and that could steer investigators down a misleading path. I'm not talking about covering up fraudulent activities — that's another can of worms; how something can be

interpreted by one person can be interpreted differently by another. You never know how a jury may interpret something.”

Increasingly emails and electronic data are scrutinized by the courts. According to *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, although email is informal, the courts are beginning to consider it somewhat more binding: Email rarely represents the “official” position of the organization. These communications reflect preliminary thought or ideas, have not been reviewed by the organization and typically only reflect the personal opinion of the parties involved. Yet, since employees of the organization created these communications, courts and regulatory agencies can construe these records to reflect the organizational view. As Deborah H. Juhnke of *Computer Forensics* puts it, “E-mail is a highly valuable source of evidence in sexual harassment cases, anti-trust cases, and other cases where casual communications take on the mantle of corporate policy” (“What Lies Beneath: Reducing Exposure in Litigation”).

When you consider that much of business transactions now occurs electronically, and corporate email use has increased exponentially in the last few years, it's understandable that electronic files and email are playing a larger role in litigation. According to IDC's third annual Email Usage Forecast and Analysis, 2003-2005, the number of worldwide email boxes is expected to increase at a compound annual growth rate (CAGR) of 138 percent, from 505 million in 2000 to 1.2 billion in 2005.

Doar estimates that “In 2003, 7 trillion email messages were exchanged by office workers in the US.” Some estimate that 70% of documents exist only electronically and are never printed in hard copy. Drafts of contracts are revised and multiple copies exist, and early drafts that may not have senior management's approval may be saved along with final drafts. “Do you want work never reviewed or approved by management subpoenaed and scrutinized in a case relating to, say, a grievance contract?” asks Neubecker. “This is why you need proactive management of data to ensure agreed upon copies of documents are retained and drafts of material that did not get by management are purged.”

“I predict over time companies and business will evolve in their use of email,” says Neubecker. “We're going to see a change in culture necessitated by document retention policies created by lawyers working with technology and risk management experts like Forensicon to develop, enforce, and audit those policies, and to educate employees on email usage. Corporations need to be prepared for this by understanding their liability and successfully managing their information archives.”