



The Seven Deadly Sins of Electronic Communications and how you can protect against them.

By Eric M. Rosenberg. LitigationProofing, LLC

www.re-soft.com
203 972 8462
info@re-soft.com

Introduction to the Problem

Everywhere you look e-mail is in the news, with many companies large and small getting into deep trouble because of it. And while e-mail and other electronic communications such as instant messaging are useful business tools, their inappropriate use has tarnished the public image of many companies and led to numerous legal problems that could easily have been avoided. Identifying potential pitfalls and taking concrete steps to prevent them can help employers save embarrassment, time and money.

The first step toward problem solution is to comprehend the principal sins of electronic communication.

1. Assuming "delete" effectively erases the e-mail trail

Despite the lessons of case after case, too many business people still believe that e-mail communications are inconsequential because they're not permanent. In fact, through technical means supposedly deleted e-mails can often be recovered. The act of erasing an e-mail is not analogous to recording over an audio or video tape and depending upon the nature of the hardware, software and skill of the forensic examiner, restoration is relatively easy. The typical sender of e-mail would be surprised at how many copies are replicated at various steps in its transmission, and we all know that we have no control over the dissemination and replication of our writing once it is on its way to a recipient.

As a matter of disaster planning and business continuity, most businesses make back-up copies of the contents of their computer systems, including electronic communications, which may be saved for months or even years. For certain businesses, such as broker-dealers and investment advisors, retention of archived electronic communications for periods of up to five years is required as a matter of law. Moreover, once an investigation or litigation is reasonably anticipated, deletion of relevant electronic communications is forbidden. For all these reasons, it's critical that business people understand that for all practical purposes their writings are permanent. By coming to that understanding, writers may indeed be more conscientious in the creation of these documents.

In addition, some inventive communication systems designed to increase productivity now inadvertently create litigation nightmares because of the persistence of the electronic record. For example, certain systems now allow employees to pick up their incoming voicemails as an audio attachment to an e-mail sent by the system to the employee's address. This means that each voicemail is saved with the same degree of permanence as the e-mail transmitting it. Imagine the expense of having to transcribe and analyze such voicemails years later when they are sought in litigation document discovery. Because of the potential permanence of any technological improvement, it is important that HR and legal departments be included in decision making about such a new system before the implementation is complete.

2. Using company e-mail for personal use

With our predilection for time-shifting and multitasking, e-mails have become the most popular means for busy people to communicate informally with friends and family, even at work. Indeed, unlike personal phone calls, e-mail cannot be overheard by colleagues, and it does not send a smoke signal to others that office work is not being accomplished. Yet the content of a personal e-mail is distinctly different from a responsible business communication. Writers of personal e-mail tap at the keyboard with relatively little forethought or restraint.

Grammar, spelling and punctuation go out of the window. Photos, cartoons, emoticons and stream-of-consciousness are typical. Since responsible employees would never dream of putting such content on company letterhead, companies should not tolerate employees broadcasting these communications on the company's electronic letterhead – i.e.: its e-mail system.

Permitting anything other than truly exigent personal use of the company e-mail system promotes sloppiness in composition of business e-mail, as writers tend to infuse their business writings with

the informality and lack of care found in their personal writings. Personal use (including betting pools, chain letters and pornographic content) can also implicate firms in improper personal behavior. Informal, anonymous surveying by this author of employee behavior has even demonstrated that a significant number of employees choose to use company e-mail systems to write and receive personal e-mail that they would not like to display to other family or friends who have access to home-based e-mail systems. Yet some of the most problematic corporate e-mails – consider the Boeing ex-CEO's alleged e-communication to a female employee, or the typical complaint to a friend about a co-worker's behavior – simply have no business being written on a company system.

Most e-mail policies make clear to employees that even their personal e-mails when written on a company system are the property of the company and are subject to company review and surveillance. In certain state and international jurisdictions it is important to publish this reminder and to have its receipt acknowledged by the employee.

3. Not considering how the e-mail would look in the public media

Even when written for legitimate business purposes, many e-mails are riddled with content never intended for newspapers or television. But that is exactly where business e-mails sometimes end up published. There is an endless supply of mechanisms by which one employee's internal or external communication can become fodder for the press. These include document discovery in litigation, freedom of information act requests in government, misaddressing, misdelivery and unexpected forwardings, and hacking.

"About 92% of Enron's e-mail database was made public by the Federal Energy Regulatory Commission and it revealed some interesting - and frightening - information: According to Audotrieve, 8% of the e-mails contained personal information about individuals, such as medications that were used by Enron employees, while another 4% contained things like offensive racial comments and pornography." (*Network World Fusion*, "Lessons from Enron e-mail database" Dec. 2, 2004).

The only safe rule of writing e-mails is this: write it as if you expect to see it appear in its entirety on the front page of the Wall Street Journal or hear it on the evening news.

4. Creating untruthful content by exaggerating, joking, losing one's temper, boasting, guaranteeing results, carrying on a debate or spreading rumors.

Remember, not everyone's humor is the same. E-mail does not convey tone of voice, even when helped along by smiley faces and other illustrative tricks. Any content that is not a true fact can be presented as supposed fact in litigation, leaving the writer with the difficult task of explaining why the exaggeration, sarcasm, or boast was included only for attention-getting effect.

The key point to remember is that in litigation, e-mail operates as a window into the writer's mind. Juries, judges and arbitrators have been known to give extra weight to content when it comes from e-mail because it is seen as an especially frank medium. One common species of joke, known as "gallows humor," is our tendency to joke about particularly difficult business problems. It, too, has all too often found its way into evidence of bad intent in civil and criminal trials. For example, in a recent federal criminal trial in Houston, the jury was required to decide whether an improper oral guarantee had been given in a purchase transaction, thus rendering the transaction a loan rather than a real purchase. The prosecutor made very effective use in his arguments to the jury of certain defendants' after-the-fact lighthearted e-mail exchange in which the word "guarantee" was used as part of the joking banter.

HR professionals have also repeatedly seen the misuse of supposed humor in electronic communications at the expense of an individual or directed at an ethnic or religious group or raising a gender issue. These e-mails are simply explosive. It takes unceasing reminders and demonstrations of the career-altering effect of these writings to put a stop to them.

Equally disturbing from a legal perspective is the tendency of electronic writers to exaggerate in order to get their messages through the electronic clutter on the recipients' machines. If the writer would not have put the same subject heading or warnings of impending doom in a memo or letter to the recipient, those words certainly should not appear in an electronic communication. Indeed, to get attention to a problem the writer genuinely believes to be serious, it is far more effective to communicate by old-fashioned hard-copy document, or by oral or written communication to company counsel or compliance personnel.

Likewise, the ease by which subjects may be casually debated through the repeated exchange of "send" buttons leads to unnecessary litigation risk. These debates tend to be less thoughtful and considered than careful memos or group meetings held to explore the pros and cons of a business decision. With the speed of light but the permanence of a backed-up hard drive, they can turn one person's idle speculation or propagation of a rumor into widely distributed mistaken statements of supposed fact.

5. Failing to heed copyright laws

When a published item is saved electronically, such as in a PDF file, you might think it's truly yours. But, the mere act of forwarding it, even internally within a company, could be a possible violation of copyright law. Company librarians can acquire certain clearinghouse rights and should be consulted before distribution of protected intellectual property. Particularly for businesses that develop and market their own intellectual property, such as firms in the entertainment industry, it is particularly unsuitable to be seen to be violating someone else's intellectual property rights

6. Failing to double-check addresses

You'd be surprised how many problems are created by employees who address an e-mail without examining the list of addressees. Doing so is quite a bit like driving a car while talking on the cell phone. You risk making mistakes without having any recollection of your actions. Be particularly mindful of the "auto-fill" function on many e-mail systems. You might be sending something to John Smyth that was meant for John Smith. Alternatively, John Smith might receive what was intended for Carol Smith. Moreover, using "Reply to All" is a bad idea, particularly if you were a "BCC" recipient. Forwarding to new recipients without a full review of the entire preceding e-mail thread also invites problems.

7. Ignoring incoming e-mail that requires corrective action

With the increased emphasis on new laws such as Sarbanes-Oxley regarding accountability and problem elevation, taking no action with respect to a problematic incoming e-mail is not a viable option. Moreover, it is usually inadvisable to solve this problem by forwarding the problematic e-mail to someone else within the company. Typically, it's a much better idea to talk to inside or outside legal counsel about appropriate handling of the problem. That step can also allow for the maximum possible preservation of corporate attorney-client and work product privileges relating to the consultation and later corrective action.

How to Prevent the Seven Sins at your Company

Having become familiar with the principal sins of e-communications, compliance and human resources personnel may be tempted to return to the days of drums and string telephones. However, there's no need to resort to that. Since any violation of e-mail policy can be costly, even a partial improvement in employee behavior will be worth the expense. Using a combination of the following techniques should produce significantly better compliance.

1. Having a written e-communications policy, signed by each employee upon hiring and updated annually, is essential.

The policy should set the standards for content and state clearly that all employee outgoing and incoming electronic communications are considered corporate property that will be subject to

surveillance and retention. The potential for discipline, including termination and personal liability to the company, should be included in the policy.

2. Content surveillance and a consistent disciplinary process should be established.

An increasing number of useful systems are available for conducting technical surveillance of company e-mail. Some of these examine communications before they leave the sender's control or before the incoming messages are distributed to the intended recipients. At best they can intercept and prevent transmission of messages that violate protocols customized for the business. Installation of a surveillance system normally involves a per-seat charge and assignment of internal compliance personnel to follow up on identified troublesome communications. Even if not perfect, the existence of surveillance, when employees know about it, should have a prophylactic effect. Indeed, anecdotal evidence suggests that the amount of troublesome e-mail declines as time goes on and employees know the standards are being enforced with state-of-the-art surveillance.

3. Employees should be required to demonstrate basic familiarity with the particular features of the e-mail system on their machines.

Without verifying an employee's specific abilities, your firm would never put an employee on a piece of heavy manufacturing or transportation equipment capable of doing great damage if misused. Similar care should be used before letting employees loose on the e-mail system, particularly since people have different proficiencies and experience with e-communication applications. It would be helpful to have a brief standardized course familiarizing every new employee with the features of your system, even producing a short test and actual "licensing" of the employee to use your system. That is far superior to the usual practice of trial and error or having a random employee give pointers.

4. Hire an expert to conduct litigation risk minimization training.

Preferably this is done in group sessions and sometimes supplemented by online follow-up. There is no substitute for demonstrating in a lecture setting the content-related problems you want to deter and connecting them to litigation issues that are not always self-evident. The process does not have to be dreary. In fact such a training session, about 45 minutes in length, can be educational and entertaining. Too many employees do not realize how their violation of any of the Seven Sins can cause problems, and how they can accomplish their missions without committing any sin. A live presentation by a skilled lecturer will allow for misunderstandings of policy to be aired and for the group as a whole to realize how their behavior must conform to standards. It also provides a good occasion for reviewing corporate policies relating to problem elevation under governance legislation (such as Sarbanes Oxley in the US) and for conveying the useful role that a company's legal staff can provide in that process.

5. Make sure that the firm's technology and legal staff are coordinating well on e-mail issues.

For example, both specialties need to have a common understanding of what retention policies are actually being enforced at the firm. New features such as voicemail delivered through e-mail should be vetted by the legal staff before they are installed.

6. Consider placing severe limits on personal use of firm e-mail and computers, cutting personal e-mails to exigent circumstances only.

One way this can be accomplished is by surveillance focused on repetitive use of non-corporate e-mail addresses. Such limitations, while perhaps initially irritating to your staff, pay large dividends by fostering discipline in the composition of e-mail content.

7. Don't save more than you have to.

Even with strong compliance training and adherence to law by its employees, a company can create unnecessary litigation expense by being unnecessarily careless in its electronic document retention practices. For example, if your company is a regulated entity, such as an investment adviser registered with the SEC, all of its business records, including e-mail, can be subject to

inspection by the regulators. Yet the SEC concedes that not all electronic communications by investment advisers must be retained under its rules. Rather, only certainly limited subject matters must be saved, albeit for a long five-year period. Under these circumstances it would make sense for any newly registered investment adviser, such as the many hedge fund advisers who recently registered for the first time, to review its e-mail retention practices in order not to store a greater electronic record than is essential for regulatory compliance.

About the Author & LitigationProofing LLC.

Eric M. Rosenberg is the president and founder of LitigationProofing, LLC. Mr. Rosenberg is a litigator with 30 years of experience, including 20 years as a manager of litigation at Merrill Lynch, as well as a frequent speaker to industry groups. This document illustrates the training and consulting services provided by LitigationProofing to financial services firms, other business enterprises, and law firms to help minimize litigation risk concerning electronic communications, attorney-client privilege and document retention. More information can be found at www.litigationproofing.com. Portions of this study copyrighted by Mr. Rosenberg have also appeared in articles written by Mr. Rosenberg for the electronic editions of Corporate Training Magazine and HR FactFinder.

About ReSoft.

ReSoft International is an independent integrator and reseller of best-of-breed software technologies that address Email & Instant-Messaging Security, Regulatory Compliance and Storage Relief.

ReSoft has, for over **11 years**, acted as a trusted advisor to hundreds of organizations, applying the relevant technologies and techniques from its broad set of Email & IM Security tools to reduce liability risks and save time.

Review the **ReSoft** website at www.re-soft.com if you are seeking ways to:

- reduce Mailbox Sizes and manage Retention & Quotas in your Lotus Domino & Microsoft Exchange systems
- undertake Legal & Regulatory Discovery Searches of Email and IM archives
- reduce Usage Violations, Loss of Intellectual Property & SPAM in Email, Webmail and IM
- make Email & IM delivery more Secure to meet HIPAA, GLB, SOX etc.
- make Exchange OWA & Outlook Calendar more Usable and Secure
- measure email/web Bottlenecks, Availability & Cost-Recovery
- proactively defend against Spyware, P2P, Worms and other emerging threats

For Further Discussions, please contact:

ReSoft International LLC
PO Box 124
New Canaan CT 06840
<http://www.re-soft.com>
203 972 8462
info@re-soft.com