DELIVERING STRATEGIC SOLUTIONS ACCA'S 2000 ANNUAL MEETING

Smart Use of Web Sites and Control of E-Mail

Presentation At ACCA's 2000 Annual Meeting

Washington, D.C.

By Micalyn S. Harris

I. Overview: The Smart Use of Web Sites

Web sites are a cost-effective way to communicate with shareholders, analysts and potential investors. Dissemination is instant and global, making worldwide publicity at minimal cost a reality. Using a web site, a company can take its road shows to dozens of locations at a fraction of the cost it would incur in visiting invitees at multiple sites. Voting via the Internet speeds tallying votes while decreasing costs. On-line shareholder meetings widen participation without significantly increasing expense. A company web site can provide numerous opportunities for publicizing information about that company's products and services, and about corporate developments. Potential suppliers, clients and customers can be directed to the appropriate individuals to contact for questions, saving company employee time and expense, thereby simultaneously increasing efficiency and enhancing goodwill.

Each of these uses has enormous potential for fast, inexpensive and effective communication. Use for securities offerings and communicating with current and potential shareholders and investors, however, also has potential has risks. Many of these risks arise from the fact that in the SEC's view, information posted on a web site (unless designated as archival or historical) constitutes continuous publication. In the absence of requiring a password or taking other measures to limit access, such publication is "general publication." Missteps in connection with such untargeted publication may subject a company to liability as a result of action by the SEC. Missteps may also provide ammunition for lawsuits instituted or contemplated by private litigants, for example, in connection with shareholder derivative suits, because company web sites are likely to be perused by private litigants and their lawyers.

As a result, companies using web sites for securities offerings, for communications with shareholders and potential investors, for advertising company products and services, and for general institutional advertising, need to consider how traditional rules will apply to electronic communications in general, and to the interplay of company web site communications and restrictions on those communications in general, and particularly while a company is in registration.

There is a continuum of risk inherent in maintaining a company web site and utilizing it for corporate communications. The first step to reducing these risks is to recognize and articulate them. The second is to decide which are worth taking in order to provide desired communication. The third is to formulate and enforce guidelines to maximize the likelihood that web site publications produce the desired results and minimize the risk of providing support for allegations of securities law violations or other unwanted results.

In general, companies use their web sites to provide two types of information: information about the company's products or services, and institutional information, that is, information about the company itself — its corporate structure and its financial structure and condition. Lawyers advising the company on securities offerings, compliance and related matters, will want to be aware of the entire mix of information available at a company's web site, but generally will focus most closely on the institutional information.

For securities lawyers advising public companies, the four most frequently asked questions regarding company (issuer) web sites are:

1. Should we post press releases? If so, which ones, for how long, and do we have a duty to update?
2. Should we link with analyst's reports about our company? If so, can we link with selected reports, either those which are favorable or those we believe are most accurate?
3. Should we host a chat room or bulletin board?
4. How, if at all, should we instruct our employees regarding participation in chat rooms and bulletin boards (the company's own, if any, and those of third parties)?

The answers to these questions must be found against a legal and technical background that is in a state of development and rapid change. The SEC's most recent Interpretative Release on the Use of Electronic Media (hereinafter, the "April 25 Release") indicates the SEC is most concerned about the risk of confusion regarding the source of information found on a company's (issuer's) web site (i.e., the company or a third

concerned about the risk of confusion regarding the source of information found on a company's (issuer's) web site (i.e., the company or a third party), and that the concern is heightened, and the appropriate standards are therefore more stringent, during a registered offering.

The SEC, however, is not the only possible critic of a company's web site management. Regardless of the SEC's views, web sites which are available to the general public are also available to plaintiffs' lawyers looking for evidence in shareholder derivative and other types of lawsuits. Therefore, in reviewing information available on a company's web site, its lawyers will want to look at the web site through the eyes of both plaintiffs' lawyers and government regulators to determine what information will be helpful and not detrimental to the company in connection with complying with applicable laws, rules and regulations, and in defending lawsuits.

II. Should You Post Press Releases?

Traditionally, press releases are published by independent third parties, either within a day or two of release or not at all. Posting press releases on a company's web site offers the company an opportunity to enhance dissemination of its press releases — a particularly valuable opportunity for smaller companies whose press releases are less likely to be picked up and published by major wire services. With the opportunity, however, comes increased responsibility. A company which can choose to post or not to post press releases assumes responsibility for assuring that what it posts, taken as a whole, does not paint an inaccurate picture of the company. Newspapers that choose to publish some press releases but not others may disregard the total picture and publish only what they deem newsworthy. A company does not have the same luxury. It may not, for example, with impunity choose to post only favorable press releases. If a company chooses to post press releases, it is well advised either to post all press releases, or have an objective policy regarding those it posts (e.g., all personnel changes above a certain level, but not plant personnel changes given only to local newspapers). A company may also wish to post information on the general scope of posted press releases. (Casting the description as company policy however is generally not recommended, as it may decrease company flexibility in changing the policy or how it is interpreted and enforced.)

In its April 25 Release, the SEC reiterated its view that posting is continuous publication, thus, by implication, raising the issue of incurring a possible duty to update. The SEC has also, however, indicated there may be some flexibility in its current position, as it recognized the potential for 10(b)-5 liability and requested comment "on how to facilitate the availability of historical information on the Internet consistent with the federal securities laws." So long as the SEC takes the position that posting is continuous publication, at a minimum, a company posting press releases will want to include warning language stating that the releases speak as of their respective dates, that subsequent developments may make the contents inaccurate or incomplete, and possibly state that the company does not have an obligation to update information in its press releases and may or may not do so. The SEC, however, has clearly warned companies that disclaimers may not be effective, particularly when sought to be used to protect a company from liability for material misstatements or omissions in violation of the anti-fraud rules.

Many companies rely on dating posted press releases and warning web site visitors that the releases speak as of their dates and may become outdated as a result of subsequent events, developments or circumstances regarding which the company may not issue a subsequent release. If a company wishes to reduce the possible risks associated with posting press releases on its web site, it may do so by establishing a policy of removing press releases to an archive or library after a set number of days, and advising web site visitors how that historical data may be obtained. Such a procedure permits press releases to remain available, but also clearly identifies potentially "stale" information as historical and not current. Alternatively, press releases may be posted for a short, pre-established period and then removed altogether.

A company may also choose not to post press releases, but if it does, it should consider whether posting press releases has become standard in that company's industry. If it is, the company may wish to indicate that it does not post its press releases, thus advising web site visitors that the absence of press releases on the company's web site does not indicate that there have been no developments worthy of or reported in press releases when in fact there have been such developments.

In addition to establishing policies for posting and removing press releases, the fact that the SEC regards web site postings as continuous publication also has implications for compliance with '33 and '34 Act requirements. For example, a company's web site should be "scrubbed" to assure compliance with '33 Act quiet period requirements, and reviewed regularly to avoid exposure to accusations that the company is, through its web site, attempting to "condition the market" for its stock.

Whether in press releases, or elsewhere, a company may find itself including forward-looking information on its web site. In order to assure that the "safe harbor" provided for forward-looking information remains available, if copies of the 10-K and subsequent 10-Qs and 8-Ks are on the web site, a link to the appropriate materials in those reports is advisable. Note that simply including a list of risk factors mentioned in the 10-K is not considered by the SEC to be sufficient to bring the company within the "safe harbor" for forward looking statements. In its April 25 Release, the SEC clearly encouraged issuers to provide hyperlinks within their own web sites in order to facilitate utilization of web site information, while, at the same time, warning that simply embedding a hyperlink within a document will not satisfy certain incorporation by reference disclosure requirements.

III. Should You Link with Analysts' Reports?

Companies that are followed by analysts and receive copies of favorable analysts' reports are often eager to link to those reports — and loathe to link to unfavorable reports. The most conservative rule for linking to analysts' reports is, don't do it, and don't provide any information about which analysts follow the company. The next most conservative policy is to provide a list of all known analysts and their identifying affiliations, but with a warning that the list may be inaccurate or incomplete, that analysts are independent and that the company takes no responsibility for their opinions or the content or accuracy of their respective reports and views.

Because the SEC has taken the position that a direct link with an analyst's report may be seen as an "adoption" of that report, linking with analysts' reports is risky. Many companies do, however, link with analysts' reports. Lawyers working in the area are unanimous in advising such companies not to link selectively. Thus, if a company decides to provide links to analysts' reports, links to all known analysts are provided. The concern here is not only with challenges from the SEC. Even if the SEC did not take the position it does regarding adoption and related issues of entanglement, linking only to favorable reports could provide a basis for plaintiffs' lawyers to argue that the company is responsible for the reports and/or that the company is conditioning the market by providing an inappropriately rosy picture.

The risk of providing links to analysts' reports can be further reduced by linking in a way which indicates, with a clear warning, that the web site visitor is leaving the company's web site, that the links are provided for the convenience of those who may be interested, that the reports are written by independent analysts and that the company takes no responsibility for their content or accuracy. The SEC remains concerned about hyperlinks from a company's web site to third party web sites, warning that "when an issuer embeds a hyperlink to a [third-party] web site within [a] document…[t]he issuer should always be deemed to be adopting the hyperlinked information." Even when the hyperlink is not embedded in a document, an issuer may be deemed to have adopted the information, and therefore responsible for its accuracy and completeness.

When a company is in registration, the SEC's concern is heightened. In its April 25 Release, the SEC warns, "statements and disclaimers will [not] insulate an issuer from liability for hyperlinked information when the relevant facts and circumstances otherwise indicate that the issuer has adopted the information."

Thus, one can envision the answer to the question "Should we provide links to analysts' reports?" as moving along a continuum of risk. The most conservative course of action is to provide neither links nor a list of known analysts at any time. The next most conservative position is to provide a list but no links, and to remove the list during registration. The next most conservative position is to provide links to known analysts reports with warnings and disclaimers, and to remove them during registration. A more aggressive position is to provide links (not embedded in a "filed" document) to known analysts' reports with warnings and disclaimers even during registration. Riskier is providing lists with no warnings or disclaimers. Riskier still is providing links with no warnings or disclaimers. Most risky is to embed a hyperlink to an analyst's report or analysts' reports in a document, as by doing so, an issuer is seen as adopting the report.

Providing links to analysts' reports or any third party web site during registration is extremely risky because one cannot control the contents of a third party web site, and therefore, cannot control the information which might be made available as a result of the hyperlink. Running the risk that one might be held responsible for the accuracy and completeness of information one cannot control, and which may change without notice, is generally an unacceptable level of risk, especially during registration. Even the most conservative position, i.e., providing no links and no list, will not however, in the absence of password protection, prevent analysts from linking with a company's web site, so including warnings, disclaimers and a notice to visitors when they enter and leave a company's web site, thus indicating what information the company controls, is highly desirable.

IV. Should You Host a Chat Room or Bulletin Board?

Chat rooms and bulletin boards are not the same. Chat rooms are real-time, on-line exchanges of messages. Content can be monitored, but not selected. Thus, content cannot be controlled until after the fact of posting. A company may, therefore, decide not to monitor, on the grounds that monitoring can impose responsibility for content which it cannot control. Not monitoring, however, may have greater risks. These include tolerating disparaging comments about the company or its products, publication of libelous materials, and including otherwise unpleasant comments which may create ill will for the company.

Because of the uncontrollable nature of chat rooms, the disadvantages generally outweigh advantages, and therefore, companies generally choose not to sponsor chat rooms unless forced to do so for competitive reasons.

Not providing a chat room, however, does not prevent the creation of ill will in the chat rooms of others. There are all kinds of chat rooms on the 'Net, and companies are increasingly concerned about what people in these third-party chat rooms are writing about them. Accordingly, companies are increasingly facing the question of whether they should spend time and money attempting to monitor third party chat rooms to find out what is being said about them, and whether, and if so, how, they should attempt to counteract "cybersmears" or stop rumors which may affect the company's stock price, product sales, or general reputation.

Bulletin boards differ from chat rooms in that messages to be posted on bulletin boards are submitted to a hosting entity and may be reviewed prior to posting. Such review can avoid a number of problems, such as foul language and libel. But it cannot avoid all problems. If the hosting entity chooses to post only complimentary information, it may be accused of not reflecting submissions fairly. Thus, even with review, a company may still find it must post uncomplimentary comments. As a result, in the absence of significant competitive pressures, most companies have opted to avoid hosting bulletin boards as well as chat rooms.

IV. Company Policies Re Employee Participation in Third Party Chat Rooms and Bulletin Boards

Lawyers and others have expressed concern that policies designed to limit employee participation in chat rooms and bulletin boards may impinge on employees' First Amendment freedom of speech, and have so far shied away from establishing guidelines regarding such participation. Employee participation in such web sites may, however, adversely affect a company, and therefore reminders of employee obligations of loyalty and confidentiality can have salutary effects simply by raising employee awareness of potential pitfalls.

For example, employees' obligations of loyalty include protecting confidential information, and avoiding contributing to discussions in ways which may give rise to rumors. An individual who is identifiable as an employee of a company (even if not identifiable as a specific individual)

For example, employees' obligations of loyalty include protecting confidential information, and avoiding contributing to discussions in ways which may give rise to rumors. An individual who is identifiable as an employee of a company (even if not identifiable as a specific individual) may be assumed to have inside information regarding its products or business, even when he or she does not in fact have such information, and comments from that individual may therefore carry unwarranted weight, or give rise to unwarranted rumors. When an employee does in fact possess confidential information, whether about the employer's products, financial situation, or other information which has the potential to impact the company's stock price, participating in third party chat rooms or bulletin boards in a manner which may disclose the employee's identity as an employee carries even greater risks.

Employees have obligations to protect their employers' confidential information. Confidential information may include trade secret information over a wide range of areas, from customer lists to financial information to intellectual property such as the subject matter of patent applications, including software and business methods. Disclosure, whether deliberate or inadvertent, can have significant adverse consequences for a company. Regular reminders of the scope of confidential information and of employee obligations to protect such information, and to be aware, at all times, of the need to avoid inadvertent disclosure, can have the salutary effect of increasing the likelihood that employees will remain aware of their obligations and meet them.

In addition to reminding employees that if they participate in chat rooms or bulletin boards they must protect their employer's confidential information, it is appropriate to remind employees of their obligations to avoid making statements which might give rise to rumors. Specific examples, such as reminding employees that chat room and bulletin board readers may know that a writer works for a particular company and conclude the writer has inside information even when he or she does not, can increase employee awareness of the scope of possible avenues for generating rumors and the range of possible issues and problems to which chat room participation can give rise. Because of the desirability of squelching rumors and dealing with damaging disclosures or disparagement, it is becoming increasingly commonplace for companies which can afford to do so, to consider monitoring chat rooms and news groups through independent third parties and to have professional public relations personnel deal with cyberspace rumors in order to attempt to reduce proliferation of unfounded rumors and minimize the impact of "cybersmears".

V. Special Issues for Broker-Dealers Participating in Chat Rooms

Brokerage firms have additional issues with which to deal when establishing policies for participation of their brokers in third party chat rooms, as well as establishing rules to assure their brokers are not participating in the firm's own chat room, lest the broker be accused of "hyping" a stock, or touting or soliciting. Brokerage firms must also deal with issues relating to the fact that certain kinds of written communications from brokers to customers must be "cleared" before sending, which is not practical for chat room participation.

Some brokerage firms regard hosting a chat room as essential to their on-line brokerage services, but are concerned about the content and course of the "chat" over which they have no control. As a result, brokerage firms that choose to host chat rooms are increasingly using independent monitors to monitor firm chat rooms. These monitors do not need to be, and generally are not, lawyers, but they do need to be trained to deal with data which has potential for stock price manipulation, hyping a stock, starting rumors, trade libel, etc.

VI. Control of E-Mail

E-mail feels like a telephone conversation. It tends to be casual, a scribbled note rather than a formal memo, and, like a telephone conversation, regarded as private. But e-mail is written communication. However beguiling its ease of use, e-mail creates a document, and depending upon internal e-mail policies and procedures, that document may or may not be handled as confidential, deemed "published" or be discoverable in connection with litigation and/or investigations by government agencies. In addition, a copy of e-mail is likely to be retained in an automatic system backup long after a hastily-scribbled note would have been destroyed. Unlike verbal conversations that are subject to the vagaries of memory, proof of what was said in an e-mail message, if it is recovered and discoverable, is relatively easy and straightforward.

Increasingly, employers are being confronted by angry employees complaining that their private messages have been read, or claiming that they have been harassed or defamed by the messages of others. Discovery requests in connection with litigation, arbitration and government investigations now routinely include requests for electronic records, specifically including e-mail, and responses have provided information which served as a foundation or corroborative evidence for claims of disclosures of trade secrets, discrimination and harassment, and anti-trust actions. People seem to make statements in e-mail communications which they would never write in a formal memo, and often make statements which they would not make in a telephone call. E-mail seems to feel private, anonymous and thus "safe" for any communication — no matter how confidential, or outrageous, its content. Thus, litigants are finding that their own and one another's e-mails are filled, depending upon their view, with land mines or gold mines.

The initial view in many, if not most companies, was to analogize e-mail to telephone communications, and permit limited personal use of e-mail in the same way they permit limited use of company telephones for personal communications. As the implications of the significant difference between ephemeral telephone conversations and the creation of a document whose exact content is retrievable came to be recognized, however, the increased risks of permitting use of e-mail for personal messages came to be recognized.

Formulating an e-mail policy is not a simple matter. If it is company policy that e-mail is to be used only for company business, then entering e-mail into evidence may also be relatively easy - either side may claim that it is a business record and entitled to be admitted into evidence as such. Alternatively, if it is company policy is to permit personal use of company e-mail, employees may feel free to send messages containing derogatory, unflattering, or otherwise unpleasant comments about co-workers that, if disclosed, may provide a foundation for claims of harassment or even defamation. Having no policy may result in realizing the worst of both alternatives.

Formulating a policy may be further complicated by the fact that in large organizations in which maintaining communications with people in distant

Formulating a policy may be further complicated by the fact that in large organizations in which maintaining communications with people in distant locations is deemed desirable (e.g. investment banking), business and social life often merge, and use of e-mail to establish and maintain contacts is encouraged. A greeting, arrangements for a dinner after work when a business trip is planned, and comparing notes on current events are often seen as appropriate uses of a corporate communications system, just as they would be appropriate uses of a telephone. Such communications are not "strictly business" but unlike telephone conversations which are not, in most instances, recorded and therefore disappear at their close, these e-mail conversations are, by definition, written records.

As a result, organizations are turning their attention to the need for e-mail policies more sophisticated than, "It's like a telephone: it is there to be used for business purposes, but we understand that you may occasionally need to make a personal call, and so long as you don't abuse the privilege, we will tolerate a certain amount of personal use."

Taking the time to develop a thoughtful policy on the proper use of internal e-mail, and implementing it with meaningful training, can avoid unpleasant and embarrassing problems. Many companies have taken the position that e-mail belongs to the company, not the employee, that e-mail is for corporate communications, and that employees cannot expect their e-mail to remain private. Whatever the company's policy, employees need to be reminded, preferably regularly, that e-mail creates a document that may have to be explained in the context of hostile litigation. Reminders of the ease of misdirecting e-mail (sometimes called the "oops effect"), and developing and maintaining systems which help avoid sending an e-mail to a group rather than an intended individual who happens to be a member of that group or whose name happens to be adjacent to the group's name, can help reduce the risk of inadvertent misdirection. (The risk exists with facsimile communications as well, but because of the widespread use of intranets providing multi-user access to documents and "broadcast" e-mail to groups of people which make it a moment's work to send out multiple copies of a given communication, the risk of misdirection or direction to an entire group instead of one member of the group, is greater than the risk of misdirected faxes or misdirected multiple paper copy mailings.)

Effective training on the appropriate use of e-mail generally includes guidance by stating principles and providing examples, and publicizing the risks and benefits of recommended uses of e-mail, together with illustrations of the undesirable consequences which may result from misuse. For example, an employee who has been advised that e-mail is monitored, that writing an e-mail message is like writing a memorandum and that language which is inappropriate in a formal memorandum is equally inappropriate in an e-mail message, is less likely to write defamatory messages or to use e-mail to harass other employees.

Software which scans e-mail for unacceptable words or phrases, for example, to reveal harassing, derogatory or libelous materials, and makes the potentially offending messages available for human review, raises another set of issues. Such review, when conducted by non-lawyer employees, may inadvertently result in waiving the attorney-client privilege by disclosing otherwise attorney-client privileged discussion to non-attorneys not involved in the matter, who arguably have no "need to know" the information and thus fall outside of the group of corporate employees to whom disclosure can be made without waiving the attorney-client privilege. Structuring the organization so that reviewing personnel are under the supervision of the legal department can reduce the risk of inadvertent waiver resulting from such reviews.

There are additional risks in using e-mail for attorney-client communications. These include potential loss of the attorney-client and work-product privileges, possible breach of the ethical obligation to treat confidential client information as confidential, and actual unintended disclosure of confidential information. Thus, additional steps to protect confidentiality may be advisable when using e-mail for attorney-client communications. Such steps include encryption, password protection, or other means of providing an additional layer of security for these messages and attached documents.

E-mail policies need to address not only the use of e-mail, but related record retention and destruction policies. Organizations often have automatic back-up systems that make and store, off-site, a copy of all electronically-stored information on a regular basis, e.g., daily, weekly, or monthly. If these back-up systems include copies of e-mail, appropriate handling of the back-up disks or tapes is also required. Even if e-mail is not included in regular system information back-ups, back-up tapes may include confidential information or trade secrets, and it is therefore advisable to handle the tapes accordingly. If back-ups are stacked where anyone can gain access to them, an argument that the information they contain is not being treated as confidential and therefore is not entitled to trade secret or other confidential status may be successful. And whether or not such tapes or disks are handled as confidential information, they may be found to be subject to discovery, and may contain relevant and damaging evidence. (Under the new Rule 26 of the Federal Rules of Civil Procedure, adopted in some jurisdictions, it may even be argued that a party litigant would be obligated to provide copies of such back-ups without having been specifically requested to do so.)

E-mail is seductive, and justifiably so. Its speed and low cost give it great potential for facilitating communications - advising businesses of opportunities and problems, and enabling them to take advantage of the former and respond to the latter rapidly. Such rapid responses make businesses more competitive, benefit customers, and reduce the duration and cost of dealing with problems. An e-mail exchange may be faster than telephone contact, and messages can travel from one problem-solver to another without a customer having to tolerate being "passed around" and encountering irritating delays.

The advantages however are not without risks. Whatever the e-mail technology, e-mail, for the foreseeable future, will create a record which, however it feels, is in effect a written record. As with any written record, the processes of creation, retention and destruction warrant attention. Policies which establish guidelines for the appropriate use of e-mail, and procedures which implement those policies by informing users of specific methods for maximizing benefits and minimizing risks, including illustrations of misuse and an indication of the problems to which they can give rise, deserve executive attention. Formulation of policies and procedures in advance can significantly reduce the risk of conflict and abuse and the attendant expenses of resolution after damage has been done. With awareness of specific technology and some advance planning, risks of misuse can be minimized and e-mail can be a valuable tool for decreasing operating costs and increasing productivity and efficiency.

VII. Summary and Conclusion

VII. Summary and Conclusion

With regard to web sites, an organization's web site which is difficult to read, difficult to navigate, and contains stale, inaccurate, or misleading information is likely to be a liability. By contrast, a web site that is visually pleasing, easy to navigate, has interesting, accurate and current information, and is easy to maintain, can be a valuable tool. Such a web site can enhance marketing the company's products and services, and enhance the reputation of the company itself by disseminating interesting and reliable corporate information and promoting good will among customers, clients, investors, potential investors and indeed, everyone who visits the site.

Similarly, inattention to the possibility that employees will be unaware of the possible impact of their participation in chat rooms and bulletin boards, or unarticulated policies regarding the use of company e-mail, can have damaging consequences. By contrast, thoughtful company policies on the use of e-mail and employee participation in third party chat rooms and bulletin boards can maximize the cost, speed and efficiency of electronic communications while minimizing the potential risks associated with careless use of the technology.

To assist in the development of establishing e-mail policies, attached are two checklists: one to assist in establishing an e-mail policy for an organization, and a second list for users.

Checklist for Organizing and Establishing an E-Mail Policy

1. Understand how the system of the organization works.
2. Emphasize that e-mail creates a document and the document is a business record.
3. Establish standards for creating, sending and accepting e-mail documents.
4. Publicize, if it is so, that e-mail may be monitored.
5. Explain the right of the company to monitor e-mail, the risk that e-mail may not remain private, and the implications of that risk for the individual users and for the organization.
6. Explain the basics of the attorney-client and work product privileges, the need to take appropriate precautions to assure that e-mail between attorney and client will qualify for protection from discovery pursuant to applicable rules of evidence. Remind users that if e-mail is discoverable and provided in connection with litigation, it may have to be explained in the environment of a hostile courtroom.
7. Establish procedures for storing and retrieving e-mail documents, including backup copies. Explain that these procedures are designed to maximize ease of use while minimizing the risks associated with that use, and deserve to (and will) be enforced.
8. Educate employee e-mail users. Merely making copies of policies and procedures available is unlikely to be sufficient. Tell "horror stories."
9. Educate clients, customers and suppliers about the organization's e-mail system with a view to reducing inadvertent abuse and assisting them in exercising good judgment regarding when and how and for what purposes it is appropriate to use e-mail and when, if at all, arrangements for using encryption or a secure socket or another method of communication are advisable.
10. Consider the advantages of encryption and of making it easily available, either by using a public-private key or other encryption scheme, or by using secure sockets for privileged and confidential communications.
11. Consider the advantages of installing a dedicated server for e-mail, and of having a separate, dedicated server for the organization's web site. The cost of the equipment is relatively low, and there are distinct advantages. These include ease of management, the ability to implement security measures (both to protect privacy and to minimize the possibility of unauthorized entry into the system), and the ability to shut down the company's e-mail system (e.g. to deal with a virus or "trojan horse" propagating via e-mail) without brining other computer-dependent operations to a halt.

Checklist for E-Mail Users

Reread Your Message. Think Before You Send. This is a document.

1. Is this a document I want to have available for unknown others to see now and into the indefinite future? If not, consider communicating by telephone. Voice conversations are ephemeral; e-mail creates a more or less permanent record.
2. Is this a message that contains information sufficiently sensitive to warrant encryption?
3. Will encryption adequately protect the confidential aspects of the message? Or will the e-mail, even if encrypted, provide clues to a reader of information I regard as sensitive or confidential, *e.g.*, that possible merger partners are having "conversation"? If so, consider communicating by telephone. The connection by telephone is direct and simultaneous. (Unintended discovery of the content of the telephone conversation would have to involve eavesdropping, via a wiretap, which is illegal in the absence of appropriate legal process. Unencrypted e-mail traveling across the Internet may be subject to legitimate review by unknown third parties.)
4. Is this a document that contains time-sensitive information? If so, consider encryption.
5. To whom is the message being sent? Have I properly coded the address so that only the intended recipient(s) are listed? Double-check addressee to assure it is addressed to the intended recipient or group, and not a larger group of which the intended recipient is a member.
6. Is this a message regarding which I wish to be able to assert attorney-client privilege, trade secret status, or other status for which encryption is likely to provide evidence of an intention to handle the message as confidential information? If so, have I included language, or provided for a password or encryption, or taken other steps to evidence that intention? Even if the only reason to encrypt is to provide evidence of an intention to handle information as confidential information, that may be sufficient to warrant encryption. What kind of a record am I building? If encryption indicates an intention to maintain confidentiality, will my failure to encrypt indicate the opposite? Cultivate consistent habits regarding treatment of confidential information.