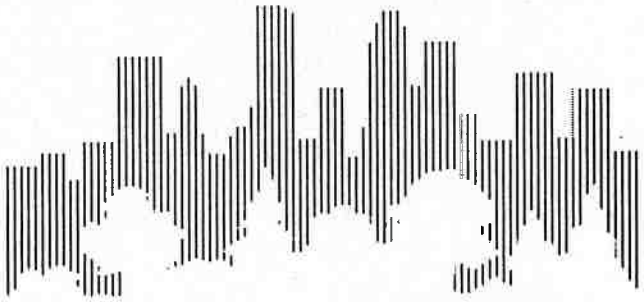
2002

# Electronic Mail: What Leaders Need to Know

Marsha J. Thiel

AUGSBURG



C • O • L • L • E • G • E

# MASTER OF ARTS IN LEADERSHIP THESIS



Marsha J. Thiel

## Electronic Mail: What Leaders Need to Know

2002

# ELECTRONIC MAIL: WHAT LEADERS NEED TO KNOW

MARSHA J. THIEL

**Submitted in partial fulfillment of
the requirement for the degree of
Masters in Arts in Leadership**

AUGSBURG COLLEGE
MINNEAPOLIS, MINNESOTA

**2002**

**MASTER OF ARTS IN LEADERSHIP**
**AUGSBURG COLLEGE**
**MINNEAPOLIS, MINNESOTA**

**CERTIFICATE OF APPROVAL**

This is to certify that the Non-thesis Project of

Marsha J. Thiel

has been approved by the Review Committee for the Non-thesis Project requirement for the Master of Arts in Leadership degree.

Date Non-thesis Completed: June 2002

Committee: Joseph A. Erickson
Adviser: Joseph A. Erickson, Ph.D.

Boyd Koehler
Reader: Boyd Koehler, M.S., M.A.

*This paper is dedicated to my children:*
*Laurie, Lisa and Christopher.*

*Thank you for your enduring support!*
*I love you!*

## ACKNOWLEDGEMENTS

I would like to thank my mentor, David M. Schultz, M.D. He understands the need for powerful technology to more efficiently manage the business of medicine. Dr. Schultz is dedicated to providing the best technology that is available, at a cost far beyond what a small organization should spend, to benefit the employees and patients of Medical Advanced Pain Specialists (MAPS). Thanks to his vision, I have the luxury of working with a technology platform that is second to none.

I would also like to acknowledge the support I have received from my Advisor, Joseph A. Erickson, Ph.D. Dr. Erickson allowed me to participate in a Computer Technology course well beyond my capabilities. He was supportive and encouraging to me as I struggled to find my way through his course. The course instilled a curiosity in me to delve further into the world of technology as it relates to the business of medical practice management. I appreciate the support and guidance offered by Dr. Erickson for this Non-thesis project.

## ABSTRACT

### ELECTRONIC MAIL: WHAT LEADERS NEED TO KNOW

**MARSHA J. THIEL**

**APRIL 2002**

Non-thesis (ML 597) Project

Electronic mail (email) was introduced to the business environment in the early 1970's. It was estimated that 130 million workers sent approximately 2.8 billion messages every day in 2000. Today, leaders all across the nation are installing email systems in their organizations. Many leaders understand the benefits but they do not understand the risks of implementing an email system. Some of the issues and risks to an organization may be: lack of "rules" for proper use, personal use on company time, perceptions of privacy, lack of confidentiality, and legal liability to the organization. Leaders may reduce the risk to their organization when installing email by: training staff on the proper use of email, educating staff on the difference between written, oral and email communication, and implementing an organizational policy for the use of email. Leaders should understand all aspects of this powerful communication tool when bringing it into their organization.

## TABLE OF CONTENTS

Page

# INTRODUCTION

"Since the advent of the Pony Express in 1860, the world has not seen a change in the method of communication that has had as much impact as the arrival of computer mediated communication (CDC)" (Greengard, 1995, p. 161). One of the most popular forms of CDC is electronic mail (email) which was first seen in the early 1970s (Fleenor & Callahan, 1987, p. 14). Even jet airplanes are hopelessly slow in moving mail across the country and across the world compared to the speed of electronic mail. Jet transferred mail has now been coined "snail mail" as it tries to compete with the concept of email. Email has changed the way people communicate (Greengard, 1995, p. 161). Time zones, postal systems and costs mean little or nothing and the technology is not intrusive like telephones. Time and distance is irrelevant. Email is faster than dialing a telephone, faxing a document or writing a traditional letter. It is not difficult to understand the allure of email in the business world.

Electronic mail was one of the first high tech management tools to receive wide publicity. Initially installed in companies with wide spans of business locations, it is now used in small companies with all employees in one site. "Today, one of the first things companies do when they get wired is get email. Securing it often comes later, sometimes after painful lessons" (Seltzer, 2000, p. 177). Email has proliferated rapidly and in many organizations no policies govern it (Greengard, 1995, p. 161; Nantz & Drexel, 1995, p. 45). In addition to making the decision to install an email system, there comes another layer of decision making for the leader. The leader must recognize the impact on the company when employees begin to use the software. Clearly, the decision to put a computer on an employee's desk may cost a lot more than the price tag of the computer.

The world is changing quickly and this presents a real challenge to the leaders of today. The technology environment is a good example of this challenge. Approximately two years ago I heard a futurist, Leland Kaiser, state that "Ninety-five percent of the technology we have today was introduced in the last 20 years (Kaiser, 1998)." Think of the burden on leaders to have the knowledge base to face this increase in technology and try to determine what is best for their company.

As a leader, I make decisions every day in a fast-paced environment. My goal is to make the best decision I can with the information I have. The challenging part of this process is to know when I have enough information to make an informed decision. Often leaders have to decide enough is enough and then be wise enough to continually evaluate what is going on with the decision and adjust accordingly.

Decision-making style of leaders varies. Leaders weigh the risk/benefits analysis and move forward accordingly to their decision making style. Regardless of their style, I believe leaders still face a dilemma regarding the implementation of technology in their workplace. I would like to suggest one solution to this dilemma. It is for leaders to share what we learn with other leaders. We can do this by networking with our professional colleagues, by publishing articles in our professional journals, and by writing papers such as this paper.

We live in a global economy and there is the challenge of business competition. On the other hand there is just the plain truth that sharing is the right thing to do. We all need each others' help if we are to optimize our work place for our business and our employees. We cannot allow each leader to learn lessons about technology the hard way – instead we need to share what we know in the new technology world. It has been said

that out of chaos comes order (Wheatley, 1992). I agree with this hypothesis. As a leader, I am finding order in the chaos but it is taking time and energy. And, in the process, staff were put through trying times that might have been avoided with proper planning and training. This paper is about sharing what I learned about the implementation of one aspect of technology – electronic mail. Some of the things I learned were learned the hard way – by making mistakes. It is not necessary for every leader to make the same mistakes.

## BACKGROUND

I am the administrator of a medical practice. I am a registered nurse by background. I have worked in the administrative area of both hospital and clinic businesses. My background could be described as clinical or it could be described as administrative. It would not be described as technical. About five years ago we made the decision to add computers to our organization. We were a new small business with a few employees working at several locations across the Twin City area. The electronic communication technology connection would allow us to communicate with staff at other sites in a timely manner. There were many decisions to be made when we decided to add technology support systems to our business. These are some of the things that we needed to decide:

- What are our business technology needs?
- What are we willing to spend for the hardware and software?
- What office software package will meet our needs?
- What hardware is needed to support the software?
- Who in the company needs the software and hardware?
- What training is needed to operate the hardware and software?

With my non-technical background, I was not prepared to answer these questions. I worked with consultants and business peers to try to find answers to the questions. After all of the hardware was installed and all of the software was loaded, it was necessary to enter user information into the system and assign various levels of security to each work group. Once set-up was completed, we needed to train the end users. We focused on what the function of each program was and how we would use the various programs within our organization. As I focused on all of these pressing decisions, I overlooked another entire dimension of issues in the decision-making and the implementation process in the email software program.

As we started to use the email software, issues began to surface. As I became more involved in the email communication concept I uncovered several potential areas of concern for our organization. This paper gives me the opportunity to share with other leaders in other organizations the things that I learned. I will outline the areas that I found necessary to understand to reduce problems and risks in the process of implementing an email system. The purpose of this paper is not to focus on the initial selection process of the various email systems that are available. I am going to move directly to the second level of thought and decision-making that should occur to successfully implement the email software and reduce the liability for the company. There will undoubtedly be items that are left uncovered in this presentation. The use of this technology is an evolving process and the discovery process will also evolve. It will be up to the leaders of this decade to define the rules for this new method of business communication. We need to understand the issues before we can define the rules.

## Statement of the Initial Problem

Although email is a method of communication that is evolving across the world, the rules are not well defined (Fleenor & Callahan, 1987, p. 14). This lack of rules became clear to me as I observed a situation in my workplace. I received an email from an employee who works in the main office of our company. He sent an email asking for my assistance. He explained that he sent an email to one of the employees in our central business office suggesting that she type her email messages in upper and lower case rather than using only upper case which was her current practice. He added to the message that using upper case only characters implies shouting and there is a term for using all caps called "flaming." She sent a reply stating that she always writes in upper case and she is not shouting. He responded by telling her that she might want to reconsider her practice because "others may misinterpret her use of upper case." She sent a message back that this was her concern, not his. And she continued to send email in upper case type only. It was at this point that I was asked to facilitate the situation. I was not an email communication expert, however, I was aware of the "rule" that upper case indicates shouting. I could not remember how I knew that piece of information. I was quite sure that it was just a tidbit of knowledge that I had come across rather than something that was formally taught to me. I sent a message to the employee who was typing messages via email using all caps. I shared with her that I agreed with the message she had received. I, too, had heard that using all upper case in a text message indicated shouting. I suggested that she adjust her style so as not to be misunderstood, just in case someone receiving her messages "also knew the rule." She did change her practice and mentioned that it would be nice to know the rules. She made a very good point!

## WHAT LEADERS NEED TO KNOW

When we installed email in my workplace, I focused the orientation/training of our email system on the hardware and software elements of the technology. I did not know the importance of focusing orientation on the actual language rules and bounds for the use of the technology communication tools. I am not alone in this omission. Although the use of email is widespread, many organizations have not yet dealt with all of the issues that email brings into an organizational communication system. We are as a society, indeed, learning a new language communication system. The last time a system of this magnitude was entered into a society may have been with the invention of the printing press or live television newscasts (Greengard, 1995, p. 161). These communication mechanisms changed the way people communicated, and email is doing the same thing today. Thus, it is important to develop and disseminate the rules for the proper use of this communication system.

"Communicative competence includes knowledge of interpretive norms that listeners can use to evaluate speech. Speech informs listeners in two respects. First, it transmits speakers' knowledge, intentions, and attitudes. Second, it provides listeners with data from which to make judgments about speakers (Bonvillain, 2000, p. 276)." Bonvillain goes on to say, "Communication competence is the knowledge of cultural rules for appropriate use of language in social interaction…Through example, prompting, and correction, they (learners) are encouraged to adopt communicative behaviors consistent with prevailing values about the propriety of expressing one's opinions, directing another's actions, or deferring to co-participants (2000, p. 299)." Learning to communicate via electronic communication tools is comparable to learning a new

language. The leader must facilitate the introduction of the rules to the employees. The leader sets the vision and the tone of how this communication system will be used within the organization. The organizational culture for use needs to be defined and taught to all staff.

As problems arose in our company, it became clear that I needed to define the vision for the use of this new communication instrument in my organization. To do this, it was important to identify the needs and the issues surrounding email. Traditional forms of communication, such as face-to-face meetings, the telephone and written communication, have specific rules of use that I believe are well understood in the workplace. Meetings take place in face-to-face communication settings. Participants are able to speak and use gestures and expressions that add to the understanding of the dialogue. There can be direct eye contact as well as vocal cues that can add to the understanding of the conversation. The telephone allows participants to hear voice and tone quality and inflection. There is interactive communication. Written communication can be in the form of memos or formal business letters. Written documents can be saved as permanent records or they can be tossed away. People in the workplace understand the rules of these communication tools. The rules for proper use are taught in school as well as on the job. There are many books written and courses taught on the topics of "effective meetings" and "business writing." My staff have demonstrated an understanding of the "rules" about oral and written communication. They understand that verbal and telephone communication is spontaneous, private and typically leaves no written record. They also understand written communication. The rules for written business communication are well defined in our organizational protocols. Employees know that the original written

documents can be filed or destroyed per company policy. They understand the privacy issues of distribution and hierarchy of inclusion in their written communication.

Email seems to be a combination of both written and verbal communication. However, there are some important differences. It was important for my staff to understand these differences. Email is quick and accessible. It is often used in a casual conversational style. However, email filters out all of the verbal cues, such as intonation and gestures, that aid in understanding the conversation. And there are different levels of understanding of the email rules (email rules are often referred to as "netiquette"). Lack of understanding on the user's part may lead to misunderstanding without awareness on the part of the sender.

Messages sent by email, unlike other forms of communication, tend to de-emphasize professional position and status (Nantz & Drexel, 1995, p. 45). The users seem to be less inhibited when communicating with superiors and across functional borders. I have observed email communication sent across two, three and even four levels of hierarchy positions on our organizational chart. It would be very unlikely to see this type of distribution pattern in a formal written document. Yet, the impact can be dramatic.

In addition to those mentioned above, there are other issues surrounding the use of email in the workplace. There seems to be a comfort level in combining personal communication in the business setting with the use of email. Employees receive email communications from friends and family on their business terminals. The staff does not seem to hesitate to spend time reading and/or responding to this type of communication. It seems that there is a lack of understanding that this is personal communication and should be done on personal time. Most employees would never dream of sitting at their

desk, taking out a piece of stationery and writing a letter to their friend. And, yet, using company time to answer personal email communication is not viewed in the same way by the staff. I realize that this attitude is my problem as a leader. I have not effectively defined the rules for this now form of communication within our workplace.

Email presents privacy issues and confidentiality issues such as who owns and may read the email on the business terminals. There is also a lack of understanding of the permanence of a document sent by email. I have an example of an email message sent by the manager of our central business office. She was concerned about how one of our physicians was coding a particular medical procedure. She stated in her email, "If this type of coding practice continues, the physician could be committing Medicare fraud." This is a very serious statement. The statement could be very damaging if presented in a legal situation during a Medicare Audit. The manager had no idea that putting this information in an email message could have grave consequences if the message was retrieved at a later date. When I spoke to her about this concept, she said, "Well, just delete the message that I sent to you and I won't do it again." This response made me realize that the employee had no idea that everything sent over our system is backed up on tape and retrievable for as long as we keep the tapes. In addition to the tape backups, the information resides on the hard drive until it is actually written over. Lack of educating employees on the permanence of email communications could have grave consequences for our business. An employee may delete a memo and assume the information is gone when, in fact, it may be retrievable.

It is important to educate the staff on the proper use of this technology to ensure that they practice the same level of high quality, interpersonal communication "on line" as they do with the written and spoken word. "The greatest skill 21st century managers will have to master is the ability to balance the driving force of technology with the universal business need to achieve results through people (Dickson, 1999, p. 27)."

In 1999, it was reported that 66 million people use email in United States corporations and that number was expected to jump to 100 million by the year 2000 (Strischek, 1999, p. 38). In spite of these numbers, only 51% reported that they had trained workers in the appropriate use of email (Strischek, 1999, p. 38). I am one of the 49% who did not initially conduct orientation sessions for the proper use of email. Nor did I define policies or procedures for the proper use of email.

I suggest leaders should take the following steps when installing email in an organization:

- orient the staff to the basic language of the email communication system
- define the rules (policies and procedures) for use of the email system
- educate the staff on the proper use of this system

Once the basic training is finished, the leader should move to the next step of training. The second step in staff orientation should focus on the language of the computerized communication system. The addition of computer technology has added several words to our language. And I am confident many of the staff do not have an understanding of the words that are used on a regular basis in our workplace. The Sapir-Whorf hypothesis states that language constructs the world in which we live. We will have cultural categories for things that are important to us (Lucy, 1992). I am definitely seeing this

hypothesis play out as I think of the words that have been introduced to our everyday business language with the evolution of computer technology. Examples of words and phrases that are now commonly used, and yet not well understood by many of the staff in my workplace, are: World Wide Web, internet, DOS, information highway, Windows, Word, Email, on-line, connected, surfing the web, web sites, internet, hard-drive, software, techies, dot-com, digital communication, chat rooms, floppy discs, c-drives, CAD, mouse, modem, CPU, RAM, ROM, bytes, list-serves, servers, viruses, search-engines, networks, megahertz, memory, programming, domain name, login, uploading, downloading, cold boot, hot swap, and browser. This is just a brief list of the new language of technology. I have included a Glossary of Terms in the Appendix A.

Leaders all across the world are installing email systems in their business (Seltzer, 2000, p. 177). Many understand the benefits, but they do not understand the risks of implementing an email system (Barker & Karcher, 1995, p. 60). This is not to say that the risks of email outweigh the benefits. It is to say that leaders need to understand all aspects of the communication tool that they are bringing into their business system. My goal in writing this paper is to share with you what I have learned about email. I hope this information will assist you in making the necessary decisions for you and your organization.

**Volume of Use**

"As of the end of 1998, 90 million United States workers were sending 1.1 billion messages per day. But by the year 2000, IDC projects that 130 million workers will flood recipients with 2.8 billion such messages per day (Dichter & Burkhardt, 1996, p. 1)." It is reported that, "Younger employees are more likely to use email. Moreover, when they

do, their messages are more likely to communicate socio-emotional content than messages sent by upper-level managers (Ku, 1996, p. 301)." It is just these kinds of messages that can create trouble, both career and legal, for the young employees and organizations. I suggest that we need to be certain these workers are using the email communication system properly for everyone's well being.

**Issues of Computer Mediated Communication**

"Unfortunately, email education and training is often focused on the hardware and software issues without regard for the requisite communication skills (Nantz & Drexel, 1995, p. 45)." I suggest that to be effective electronic communicators, employees need training in understanding the issues surrounding email. And I believe many employees do not understand the ramifications of sending and receiving messages on organizations' computer resources. Although email has unprecedented speed and efficiency, it lacks the visual or audio feedback of face-to-face or telephone communication. It lacks the rules of conduct and special language rules to meet the unique requirements of computer-mediated communication. It seems some of my employees find email use to be frustrating and too foreign to their routine methods of communicating. As a result, I have observed staff being hesitant to use the system. I found that assisting staff to understand these issues helped them deal with their fears. Investment in advanced technology may not necessarily result in improved communication in the workplace if use of the tool is not properly taught.

"Electronic communication may cause a major change in the organizational communication process because senders can circumvent traditional communication

hierarchies (Nantz & Drexel, 1995, p. 45)." To avoid this problem, each organization should define appropriate communication lines for email communication distribution.

"Industry experts are predicting that junk electronic mail volume will increase astronomically in the next decade and will far outweigh the volume of junk surface mail because the advertisers are using wide-area networks like Internet mass marketing strategies at little to no cost (Nantz & Drexel, 1995, p. 45)." This presents a time issue as employees need to wade through the tremendous amount of email coming into their systems. It is risky to assume that an incoming message is junk and delete it without reading. Thus time must be taken to look at each incoming message. There are ways to program email software to automatically delete junk email.

**Liability Issues**

Leaders need to be aware of the possible liability exposure and control concerns related to the adoption and use of email. Once informed, leaders can then establish email policies that balance organizational goals and the need for effective controls with fairness to email users.

I suggest that the protocol and procedure for backing up and storing data should be defined by each organization. You should define how often backup tapes are run, where they are stored and how long they are kept. You should also define when information is purged. Every user needs to understand that delete does not necessarily mean delete. "Email messages that are 'deleted' (i.e., clicking on a delete button with the mouse) may not necessarily be inaccessible or unretrievable. Consequently, 'deleted' email messages may still be subject to a discovery request. Specifically, if information that has been 'deleted' has yet to be overwritten by the computer system or is stored on backup tapes or

archive tapes, the information may still be accessible (Dichter & Burkhardt, 1996, p. 18)." There is a kind of informality to email that seems to encourage candor and off-hand comments. Thus, when an employer becomes involved in litigation, email is a fertile filed for the discovery process for the prosecuting attorney (Dichter & Burkhardt, 1996, p. 18). Users of email are often unaware that deleted messages are in fact still available for months or longer in a computer's hard drive or on a back up tape or disk. Therefore, the messages can be retrieved months after they were deleted in the event of litigation. And even if you delete and provide assurance that the message is gone, it does not mean the recipient deleted the same message.

Unfortunately, derogatory email evidence may be just the proof that prevents a court from buying the employer's articulated reasons for the action challenged in the lawsuit (Ditcher & Burkhardt, 1996, p. 18). This concept has spawned a new industry of computer sleuths who help lawyers find incriminating evidence in computer files. The "deleted" email messages can become the smoking gun of litigation. If your files are subpoenaed, the investigators may come into your business and seize your computer hardware, software and files (Ditcher & Burkhardt, 1996, p. 18).

**Privacy Issues**

"Most of the risk involved in the use of email centers on the issue of privacy. In the United States, the Supreme Court has been called on to interpret the Fourth Amendment's guarantee of privacy in novel ways, especially as the technologies for the transmission of information emerge. For example, the court has ruled that citizens have the right of privacy from invasion of their phone calls or mail. The rights of the organization and those of the employee may be in conflict with respect to the privacy issue (Barker &

Karcher, 1995, p. 60)." In my opinion, most managers would agree that neither a person nor an organization should be allowed to intercept or peruse an individual's private property. This forces the question of ownership. Who owns the property inside the company-owned computer? Since the computer is an asset belonging to the company, one could argue that company representatives are entitled to review files within the computer. Conversely, the employee may expect personal messages transmitted via email to be afforded the same right to privacy granted for telephone conversations and personal mail.

"Employees' right to privacy is governed by Electronic Communications Privacy Act of 1986 (ECPA) and state tort law. Section 2701 of ECPA makes it a federal offense, subject to a penalty of up to $250,000 and imprisonment, for an individual to read someone else's email (Riddle, 1988, p. 7)." The ECPA applies to communication passed over public lines, which excludes any communication within a single business organization. Judges have ruled that organizations are legally responsible for electronic messages sent by employees (Nantz & Drexel, 1995, p. 47). The ECPA sets minimum standards for email privacy that state laws may exceed and supercede. Coverage by state law could be complicated by the fact that so many messages are sent across state and even national boundaries.

The Pillsbury Company in Pennsylvania was one of the first companies to test the laws of privacy regarding email.

> "In one of the first cases to address the privacy rights of employees with respect to email messages the federal district court applied Pennsylvania state law. *Smyth v. The Pillsbury Co.* . . . In *Pillsbury,* the plaintiff,

> Michael A. Smyth, was an at-will employee who received certain email messages on his home computer from his supervisor over defendant's email system. He then exchanged emails with his supervisor, which contained offensive references and threats concerning the company's sales management . . . Company executives, who saw a printout of this message, then read all of his email messages and terminated him for inappropriate and unprofessional comments over Defendant's email system . . . The court, taking a broad approach, found that there is no reasonable expectation of privacy in email communications voluntarily made to a supervisor over a company-wide email system despite the fact the employer assured the plaintiff that the email messages would not be intercepted by management (Ditcher & Burkhardt, 1995, p. 4)."

Some states have ruled it illegal to eavesdrop on private conversations or phone calls made on company phones; the employee's expectation may be that the same privilege will extend to email (Barker & Karcher, 1995, p. 62). However, in a recent suit against Epson Corporation in California, "The court ruled that California privacy laws do not extend to workplace surveillance (Barker & Karcher, 1995, p. 62). Keep in mind, if you have a multi-state operation, it is important to be familiar with the laws in each state in which you have employees.

There are issues regarding definition of computer privacy. I suspect these issues will resolve as we learn more about the technology and see the issues play out. Jerry Berman of the Civil Liberties Union states, "The issues are going to be decided partly by the courts, partly by the Congress, and partly by the institutions developing a culture around

these technologies (Goode and Johnson, 1991 p. 8)." As with anything new and unfamiliar, legislatures struggle to keep up with the laws needed to govern issues surrounding technology.

In addition to privacy, the security issues are another major concern. Moving information over lines places companies at risk for people outside the company to intercept company information. This may be a serious concern for organizations that must ensure privacy of their information. Examples of areas that need assurance of privacy are transmitting charge card information or the transmission of medical information. Encryption programs allow the sender of an electronic message a degree of privacy. Pretty Good Privacy (PGP) is a trademarked program for encrypting messages so that only the intended recipient can read the messages (PGPI, 2002). The program provides protection against anyone tapping in on the network. Even if the message is intercepted, it will be unreadable to the intruder. PGP allows for message authentication. Authentication, through a system referred to as digital signature, ensures that a message appearing to be from a particular person can have originated from that person only and that the message has not been altered. PGP can be obtained free for non-commercial purposes.

**Personal Use**

A potential issue facing organizational leaders is the personal use of email on company time. Leaders in an organization may have conflicting views from their internal decision-making group regarding how to address this issue. This is an issue I deal with in my organization. Some directors allow staff to use their own professional judgment as to how much time they spend on personal use of the email system. Other directors believe

that employees should not be allowed to use business time for personal use. Some are concerned that enforcing a no-personal-use policy may alienate the staff or lower staff morale. They report that employees are working long hours and may enjoy the perk of tending to some of their personal business at their desk. The philosophy on personal use of email needs to be defined by each organization.

Coming to agreement within the organizational leadership group may be a challenge. It is important to balance the cost benefit of the policy decision for your organization. Employee use of the company email network for private communication creates a cost issue for the organization. Denial may become a morale issue. While the marginal cost per message may appear to be minimal, it is important to actually compute the cost. Imagine if, for example, each of your employee email users sent or received several personal messages per day. Let us look at an example of impact. We will say the average time to read and respond to an email is one minute. If an employee receives and replies to five personal emails per day at one minute per email it amounts to five minutes per day per employee. If you have an organization of 100 employees and each employee spends five minutes per day on personal email time you are losing 1.0 full time equivalent (FTE) per day in employee productivity. (60 minutes per hour X 8 hours = 480 minutes work time per day. Personal email time of 5 minutes per day X 100 employees = 500 minutes per day of personal email time. 500 personal minutes divided by 480 total minutes per day = 1 FTE per day). A leader needs to consider this information when defining the personal use policy for email. Things to consider when defining your policy include whether the employees are salaried or hourly employees and what the typical workday demands are for the staff.

I suggest that an organizational policy that permits incidental and occasional use of email for personal communication leads to staff satisfaction especially if the staff understands the cost of regular use for personal business. Show the above calculations to your staff. I believe employees want to do what is right and if they are given the information to understand the ramifications, the issue may take care of itself.

**Computer Viruses**

A virus is a piece of software that is written to adversely affect your computer without your permission or even your knowledge. It is a piece of program code that implants itself to an executable file and spreads systematically from one file to another doing damage along the way. Computer viruses do not spontaneously appear; they are written to have a specific purpose.

You cannot get a virus or any system damaging software by reading the actual message in an email. Viruses do not exist in the text portion of the email. Viruses must be attached to and infect an executable program (.exe). Viruses only exist in executable files; email is not an executable file. While reading email you would not be executing a malicious virus code. However, if you download a file attached to an email and open it, there is a chance that the attached file could contain a virus. For this reason it is important that you do not allow your email program to automatically open an attached file. Viruses are usually operating system-specific. In other words, viruses created for a DOS application can do no damage on a Macintosh operating system and vice-versa.

To reduce your risk of being infected with a computer virus install an anti-virus program such as Norton Virus Scan or McAffee Anti-Virus software. Be sure to note that these programs need to be updated on a regular basis to ensure protection for your

system. Antivirus software will not detect a virus until it has been programmed to do so; thus, the first round of a virus will do damage until it is reported and code is written to stop it from spreading. This code needs to be installed as an update in your software to be effective. The easiest way to avoid a virus is to not run attachment programs. This may not be practical in your organization. It is possible to block .exe files from being distributed to your staff. The .exe files are held by the system. The employee is notified by the system administrator program that the file came in but was not delivered. You may limit your exposure by adding a statement to your policy that employees are not allowed to open attachments that are not business related.

**Storage Space**

Storage space on server is another challenge for your business system. It is important to understand the amount of space that seemingly innocent emails can take up on your server. It is an issue especially if the employees distribute their files to other staff. I see this apply most often to the cute cartoons and jokes that are distributed in our office. One staff member may receive an email they think is "cute" and decide to send it to others within our company. If each person who receives the message decides to save it into a file it can take up a lot of space on the main server. Educating staff on this concept may help reduce the scope of the issue. I will give one example. One person in our office received a small, animated cartoon. The size of the cartoon file was 220 kilobytes. The employee forwarded the cartoon to a group of 60 people in our office. Now the cartoon is taking up 15 megabytes of storage space on our server. Our total server space is eight gigabytes (8,000 megabytes). If one small cartoon takes up 15 megabytes of space, you can see how this could be a great drain on a system if not properly managed.

## Listservs/Discussion Groups

In addition to using email for business or personal correspondence, there is another way to benefit from email. This is to participate in an electronic discussion group. Electronic discussion groups are also known as listservs. Listservs allow people with similar interests to communicate on a topic and share ideas amongst the group. Messages are posted to all members of the discussion group. Some listservs are monitored by people (moderated); others are simply computer-mediated with no human involvement (unmoderated). All messages sent to the discussion group are forwarded to all members of the group. Any person who is a member of a listserv group can participate by reading and responding to any messages posted to the group. This is a good way for professionals who are all across the country, as well as the world, to connect and communicate with each other. These groups allow the participants to be aware of the latest developments in their specialty. They also allow you to ask questions and share your expertise on a particular topic. It is a good idea to read the postings for a couple of weeks to get an idea for what is acceptable use of the list before you enter into the discussion (Erickson, 1999).

## Policies for Use

Email is a great business tool. However, it can present significant risk for employers. It is important for a leader to be aware of the various types of risk. There can be legal liability for any content produced on the software, breaches in confidentiality surrounding propriety business information, perceived invasion of privacy on behalf of the employees, lost employee productivity and damage to the reputation of your business. One way to

begin to manage these threats is to develop an email policy for your organization. A simple and clear policy that everyone is aware of is the best approach.

After the employees review the company policy, they should sign a statement that they are aware of and understand your policy. The case of *Bourke v. Nissan Motor Corporation* demonstrates why this is important:

> "A woman was conducting a training session demonstrating the use of email at a care dealership. She randomly selected a message sent by an employee of the Nissan Company to an employee of the dealership. Unfortunately, the message was personal, sexual and not at all business-related. Later, after being terminated for poor performance, the Nissan employee sued for invasion of privacy . . . a California court of appeal ruled that the Nissan employee had no reasonable expectation of privacy because she had signed a statement restricting her email to company business (Nolo, 2002, p. 2)."

It is important for employees to understand that deleted does not necessarily mean non-retrievable. Deleted items can remain in the system long after the original writer deletes the memo. The deleted items may be retrieved by experts at a later date. These items can be damaging to an organization especially during the course of a lawsuit. "For example, when government lawyers sued Microsoft over antitrust issues, some of the most incendiary evidence came from archived emails that documented statements by Microsoft executives about its strategy against competitors such as Netscape (Nolo, 2002, p. 4)."

In the absence of a notice to the contrary, employees tend to perceive email as private and think the messages belong to them. System security features (such as personal

passwords) reinforce this illusion of privacy. Policy statements should inform the employee that hardware and software are the property of the employer. As such, the employer has the right to read or monitor any and all information on the system. Electronic monitoring is defined as reading, listening to, or otherwise monitoring employees' written, oral or electronic communications. If you plan to monitor your company email use, it is critical to include this information in your policy. The best privacy policy statement, in my opinion, lies somewhere between the two extremes of total employer control and total employee privacy. In any case, the policy should be enforceable and fit the company culture.

Employees should not only be informed about policies regarding privacy in the use of email; they should also be instructed on how email should be used and what types of subjects and language should not appear in the system. I chose the following guidelines for using our system based on previously developed general policies for our company's acceptable organizational behavior. Email should not be used for commercial ventures, to encourage religious or political causes or to benefit any organization not affiliated with the company. Messages containing insensitive language, racial, sexual or ethnic material is not acceptable. Email should not be used to transmit material that is offensive, abusive, contains obscene or vulgar language, gossip, ridicule or retaliatory messages.

Having a policy is one thing, but having the ability to enforce it is an entirely different issue. If employees know email is not private and it may be read by superiors, this knowledge alone may eliminate any problems. I included a statement that misuse or abuse of the email system will result in discipline up to and including termination.

Problems with developing and implementing your company policy may arise if a balance between the employees' right to privacy and the company's need-to-know is not achieved. Doing what is right for the employer and the employee is the balance that needs to be found for personal use of the email system.

The specifics of each organization's email policy will obviously vary. When you are developing your policy, consider and answer the following points:

- Privacy: Must the organization obtain consent from the employee before accessing organization records under the employee's control? May the employee request email privacy?
- Legal Issues: Does the policy comply with the applicable local and state legislation?
- Past Practices: What rules are in place with regard to personal use of the organization's traditional or electronic communication networks? Are the rules governing email consistent with other forms of communication and record keeping within the organization?
- Permissible Use of the Email System: Under what circumstances, if any, may the system be sued for non-company business? Will non-company use be subject to a different level of monitoring?
- Company Monitoring Policies: How will email be monitored, with what frequency, and by whom? Will just the existence of the message be monitored or will monitoring include checks of message content? Will employees be notified when monitoring is taking place?
- Enforcement: Is the policy practical and enforceable?

- Dissemination: Have all interested parties been informed about and consented to the policy? (Barker et al, 1995, p.63).

Once the policy is developed, it must be explained to the employees. Be sure to have the employees sign a statement saying they have read and understand the company policy. Keep the signed statement in the employee personnel file. If the leadership team defines the company policy, informs employees of that policy, and then follows the policy, the likelihood of privacy issue lawsuits should decrease. I have included a sample of the employee letter and the policy developed for my organization in Appendices B and C.

## EMAIL TRAINING INFORMATION

In addition to training staff about the mechanics of using the hardware and software for email, leaders also need to train the staff about the proper use of the product. There are several areas that leaders may want to understand in order to plan training sessions for your staff. If an employee understands the proper use of the software you may avoid some of the issues that I encountered prior to implementing our educational program.

### E-Mail Etiquette (Netiquette)

Employees who have not received training on the proper use of email may not understand the concept of email etiquette. Proper use of the software requires understanding the rules. Those who know the rules are frustrated by those who do not know the rules. As I described in my workplace example, the employee who understood the rules of etiquette negatively judged the employee who violated the email etiquette rule, even though the violation was done without any awareness. The novice email users who do not follow the etiquette are known as a "newbies" or new users. They should be

treated kindly. I suggest that it is the leader's responsibility to know the rules and teach proper use of the system. There are several on-line sites to assist you. Arlene Rinaldi hosts a popular netiquette web site. I have included Rinaldi's set of netiquette rules taken from a document prepared by Rinaldi (1998) that defines email guidelines and netiquette:

- Under United States law, it is unlawful "to use any telephone facsimile machine, computer, or other device to send an unsolicited advertisement" to any "equipment which has the capacity (A) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper." The law allows individuals to sue the sender of such illegal "junk mail" for $500 per copy. Most states will permit such actions to be filed in Small Claims Court. This activity is termed "spamming" on the Internet.
- Never give your user ID or password to another person. System administrators that need to access your account for maintenance or to correct problems will have full privileges to your account.
- Never assume your email messages are private nor that they can be read by only you or the recipient. Never send something that you would mind seeing on the evening news.

- Keep paragraphs and messages short and to the point.
- When quoting another person, edit out whatever isn't directly applicable to your reply. Don't let your mailing or Usenet software automatically quote the entire body of messages you are replying to when it's not necessary. Take the time to edit any quotations down to the minimum necessary to provide context

for your reply. Nobody likes reading a long message in quotes for the third or fourth time, only to be followed by a one line response: "Yeah, me too."

- Focus on one subject per message and always include a pertinent subject title for the message; that way the user can locate the message quickly.
- Don't use the academic networks for commercial or proprietary work.
- Include your signature at the bottom of Email messages when communicating with people who may not know you personally or broadcasting to a dynamic group of subscribers. Your signature footer should include your name, position, affiliation and Internet and/or BITNET addresses and should not exceed more than 4 lines. Optional information could include your address and phone number.
- Capitalize words only to highlight an important point or to distinguish a title or heading. Capitalizing whole words that are not titles is generally termed as SHOUTING!
- *Asterisks* surrounding a word can be used to make a stronger point.
- Use the underscore symbol before and after the title of a book, i.e. _The Wizard of Oz_
- Limit line length to approximately 65-70 characters and avoid using the enter key.
- Never send chain letters through the Internet. Sending them can cause the loss of your Internet Access.

- Because of the International nature of the Internet and the fact that most of the world uses the following format for listing dates, i.e. MM DD YY, please be considerate and avoid misinterpretation of dates by using other formats.
- Follow chain of command procedures for corresponding with superiors. For example, don't send a complaint via Email directly to the "top" just because you can.
- Be professional and careful what you say about others. Email is easily forwarded.
- Cite all quotes, references and sources and respect copyright and license agreements.
- It is considered extremely rude to forward personal email to mailing lists or Usenet without the original author's permission.
- Attaching return receipts to a message may be considered an invasion of privacy.
- Be careful when using sarcasm and humor. Without face-to-face communications your joke may be viewed as criticism. When being humorous, use emoticons to express humor. Emoticons are symbols used to illustrate emotions in the absence of body language and voice tone. For example: : - ) is a happy face for humor (tilt your head to the left to see the emoticon smile).
- Acronyms can be used to abbreviate when possible; however messages that are filled with acronyms can be confusing and annoying to the reader. Examples of acronyms are:

- IMHO= in my humble/honest opinion
- FYI = for your information
- BTW = by the way

**Guidelines for Use**

Each organization should develop guidelines to help the users select the appropriate communication tool. I teach that email is appropriate for a message that is informal, needs to reach multiple people and get to the receivers quickly. If the information is a document that needs to be formal, secure and permanent, email is not the correct choice in my organization. These documents need to be printed and distributed. I do make one exception – if the document needs to be distributed quickly to multiple sites, the writer may send the document as an attachment in "Read Only" format and follow it with a paper document. (Read only format allows receivers to read and print the document but they do not have the ability to edit the document). The leader should define the protocols and communicate the protocol to staff.

**Proper Email Format and Structure**

Software for creating email provides a template for most elements of format, but writers must also be attentive to structuring their messages correctly. Users should understand the following information:

- Recipient's Address – must be letter perfect. A misspelled email address will result in one of two situations: the message will be returned to the sender with the notations that "no such user" was found at the intended site or the message ends up in the email box of the wrong person. Unlike a misaddressed envelope that can be returned to sender without being opened, an email message is typically read

before the mistake is discovered. Email addresses within a company may follow a naming convention pattern – don't assume it is so and guess at an address unless you send a "test" to be certain you are reaching the proper address. There may be several J Andersons in one company.

- Date and time are automatically generated in the email software. Be sure the system clock of your computer is correctly set.
- Subject line. An effective subject line attached to an email message puts the reader in the right context to receive the message.
- Mark the email urgent if it is important that the receiver read it immediately. Do not overuse this preface. However, urgent email has no priority in arrival or listing order over other email coming into your system.
- Email messages should be signed appropriately. Select your salutation based on type of message and relationship of participants. For business correspondence, end with a signature block that contains the sender's name, title (If appropriate), company, phone number and email address.
- Message length – messages should be concise and focus on a single subject. Researchers recommend that messages not exceed 25 lines, the amount that fills the typical screen. Limit line length to 75-80 characters since older email software sometimes does not automatically wrap text. Writers may find that the end of their sentences are truncated. This problem will disappear as newer software is more widely adopted. Avoid making the receiver scroll from left to right to read your message.
- Organize your thoughts.

- Use spaces instead of tabs for indenting because the receivers tab settings may be different. This may cause the layout of the message to become distorted which is difficult to read.
- Use only standard ASCII characters and system fonts rather than fancy, elaborate type. Your receiver may not have the fancy fonts.
- If you are attaching a document, check it for grammar, punctuation, spelling, sentence structure and other errors before sending it.
- Be careful with the reply button. Be sure you are sending to the right person or group of people.
- When attaching documents find out what software the receiver has so the file can be sent in the proper format. For instance, if you send a Power Point presentation and the receiver does not have Power Point, he cannot open the file.
- Do not send information that you would not want posted on the bulletin board. Remember, Bill Gates, the creator of Microsoft, had his email subpoenaed.
- Attachments may contain viruses. Scan before sending a file and before opening an attachment that is incoming. Know your policy regarding which attachments you can open.
- Use emoticons sparingly or not at all. The term emoticon comes from Emotions and Icon. They are used to illustrate emotions in the absence of body language and voice tone. I have included a list of emoticons in Appendix D.
- Do not send duplicate copies or forward copies of private email without the permission of the writer.

- Do not send unsolicited mail, such as chain letters and junk mail (Extejt, 1998, p 58-60; Goode & Johnson, 1991, p. 64).

**Pearls of Wisdom**

Email shares the temporary, convenient, and volatile attributes of telephone or spoken conversation, but at the same time is as permanent a medium as the written word. As I prepared this paper, I came across several concepts that I think are important. I would like to share them with you:

- In order to be an effective communicator you must anticipate and meet the needs of the receiver by using language the receiver will understand by providing the information the receiver needs and providing psychological support the receiver needs.
- Answer communication promptly or in a timely manner.
- Do not ask for something in an email that you would not request in person.
- Avoid sarcasm and too much humor because both can be easily misinterpreted without the aid of body language.
- Be sensitive to people from other countries and cultures.
- Make sure you are not sending a message that you will regret later. Nobody has regretted not sending something inflammatory. Plenty of people have regretted messages they have sent in a moment of anger. One of the problems with email is that it is easy to get nasty with someone who is nothing more than a name on a computer screen. That message could come back to haunt you. A receiver can save it, forward it or print it out and distribute it.

- If a message is being written in anger, do not send it without rereading it for tone and content. Preferably, put it away for a few hours and then reread. Once an email is sent you cannot retrieve it.
- Be especially careful about what you send. Email provides an illusion of privacy, but not the reality of privacy. Once the email is sent the author has no assurance of confidentiality or ownership.
- Encourage employees to use the same degree of care in writing email as they would in drafting a letter on company letterhead. Avoid "off the cuff" comments that would not reflect favorably on the company if disclosed. The words of the sender reflect on the company even if the company states a disclaimer.
- Follow the proper chain of command when you correspond with people within your company. Do not send email to the president of the company just because you can.
- Don't assume that every email message reaches its destination.
- You may need to notify your family and friends that they should not send personal email to your work. Set up an email account at home for your personal communication needs.
- Email messages are easily redistributed in original or an altered form. With the push of a button or the click of a mouse, a message the sender intended as personal can be broadcast to hundreds of people around the world.
- If you receive an attachment you do not understand or are not expecting, send an email back to the sender and ask what is in the attachment. If it is a document you

are supposed to receive, the sender will tell you. If not, delete it immediately. You may avoid opening a virus-infected file that will damage your system.

- Remember "Delete" does not mean gone!

## SUMMARY

Computers with network connections make it possible to communicate globally and instantly with anyone who has similar technology. Technology offers wonderful opportunities for team members to work across borders, spending time together on projects without ever meeting face to face. Computer networks, the internet and wide use of email that let people from around the world work together on projects will not, in and of themselves, ensure that these projects will be successful. Leaders and their teams must be able to communicate effectively in person and on line.

Email is a business tool. It requires knowledge and expertise for proper use. It is essential people learn how to manage it. It is the leader's responsibility to ensure the staff understand and follow the proper use of email in each organization. It is my hope that the reader will receive information and guidance in this document to help carry out this mission.

## REFERENCE LIST


Barker, R., Karcher, N., & Meade, N. (1995). Email issues. *Internal Auditor, 52,* 60-64.

Bonvillain, N. (2000). *Language, culture, and communication: The meaning of messages.* New York: Prentice Hall.

Caudron, S. (2000). Virtual manners. *Workforce, 79,* 31.

Dichter, M., & Burkhardt, M. (1996). *Electronic interaction in the workplace: Monitoring, retrieving and storing employee communications in the internet age.* [Electronic version]. Retrieved February 15, 2002 from http://www.morganlewis.com/art61499.htm

Dickson, C. (1999). Forecasting business communications for the 21st century. Pittsburgh *Business Times, 19,* 27.

Erickson, J. (1999) *Threaded discussions.* [Electronic version]. Retrieved September, 1999 from http://www/augsburg.edu/education/mal599/lesson6.html

Extejt, M. (1998). Teaching students to correspond effectively electronically. *Business Communication Quarterly, 61,* 57-68.

Fleenor, C., & Callahan, R. (1987). Managing the technology of communication. *PC Week, 4,* 14-16.

Goode, J., & Johnson, M. (1991). Putting out the flames: The etiquette and law of email. *Online, 15,* 61-66.

Greengard, S. (1995). Email: Using your connections. *Personnel Journal, 74,* 161-166.

Kaiser, L. (1995). *Technology and the future*. Presentation at Twin City Medical Management group.

Ku, L. (1996). Social and nonsocial uses of electronic messaging systems in organizations. *Journal of Business Communications, 33,* 297-325.

Lucy, J. (1992). *Language diversity and thought: A reformulation of the linguistic relativity hypothesis.* Cambridge: University Press.

Nantz, K., & Drexel, C. (1995). Incorporating electronic mail into the business communication course. *Business Communication Quarterly, 58,* 45-52.

NOLO Law for all. (2002). *Email privacy.* [Electronic version]. Retrieved March, 2002 from http://www.nolo.com/lawcenter/ency/article.cfm

PGP (2002). *Pretty good privacy encryption software.* [Electronic version]. Retrieved February 15, 2002 from http://www.pgp.com/products/freeware/default.asp

Rinaldi, A. (1998). *The net: User guidelines and netiquette.* [Electronic version]. Retrieved February 15, 2002 from http://www.fau.edu/netiquette/net/bib/html

Riddle, M. (1988). The electronic communication privacy act of 1986: A layman's view. [Electronic version]. Retrieved March, 1999 from http://193.2.1.68/ECPA_layman.html

Schwalm, K. (1997). *A quick and dirty guide to email terminology.* [Electronic version]. Retrieved February 15, 2002 from http://gcinfo.gc.maricopa.edu/~schwalm/email/guide.html

Seltzer, L. (2000). Secure email. *PC Magazine,* 177.

Strischek, D. (1999). Email communication: Some rules of the road for the information superhighway. *The Journal of Lending and Credit Risk Management, 81,* 38-44.

Vincent, A. (1999). Business communication: Are the rules different for email? *Supervision, 60,* 10-15.

Wheatley, M. (1992). *Leadership and the new science: Discovering order in a chaotic world.* San Francisco, CA: Berret-Koehler Publishers.

## APPENDIX A

## GLOSSARY OF TERMS

This Glossary of Terms was borrowed from A Quick and Dirty Guide to Email Terminology at http://gninfo.gc.Maricopa.edu/~schwalm/email/guide.html 2002

**asynchronous communication**

Computer-mediated exchanges of messages when the participants are not on-line at the same time. These discussions are drawn out over time, and the participants read and respond as their schedules permit.

**browser**

A browser is a program that provides a way to look at, read, and even hear all the information on the World Wide Web. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files on-line. By the time the first Web browser with a graphical user interface was invented (it was called Mosaic), the term seemed to apply to Web content, too. Technically, a Web browser is a client program that uses the Hypertext Transport Control Protocol (HTTP) to make requests of Web servers throughout the Internet on behalf of the browser user.

Currently, the most popular browser is Netscape Navigator. Microsoft's Internet Explorer is gaining usage as Windows 95 installations grow. A commercial version of the original browser, Mosaic, is still widely used. Other browsers include the browsers for the on-line services, America On-line, Compuserve, and Prodigy, but these are beginning to offer Netscape or Internet Explorer in addition to or as a replacement for their own. Lynx is a text-only browser for UNIX shell and VMS users. ÊiWorld, an electronic newspaper on the Web, provides a great deal of information about browsers and their usage on their BrowserWatch pages.

**client**

A software program that is used to contact and obtain data from a server software program on another computer, often across a great distance. Each client program is designed to work with one or more specific kinds of server programs, and each server requires a specific kind of client. A web browser is a specific kind of client.

**e-mail (electronic mail)**

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. Messages are encoded in ASCII text. However, you can also send non-text files, such as graphic images and sound files, as attachments sent in binaryÊstreams. E-mail was one of the first uses of the Internet and is still probably the mostÊpopular single use. A large percentage of the total traffic over the Internet is e-mail. ÊE-mail can also be exchanged between on-line service users and in networks other thanÊthe Internet, both public and private.

E-mail can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an e-mail reflector. Some mailing lists allow you toÊsubscribe by sending a request to the mailing list administrator. A

mailing list that isÊadministered automatically is called a list server. E-mail is one of the protocols included with the Transport Control Protocol/InternetÊProtocol (TCP/IP) suite of protocols.

Among the more popular e-mail programs are Qualcomm Communications' Eudora and Connectsoft's E-Mail Connection, a shareware program.

**gateway**

The technical meaning is a hardware or software set-up that translates between two dissimilar protocols; for example Prodigy has a gateway that translates between its internal, proprietary e-mail format and Internet e-mail format.

Another, sloppier meaning of gateway is to describe any mechanism for providing access to another system, e.g. AOL might be called a gateway to the Internet.

**groupware**

Groupware refers to programming that supports people working together in a collective effort but located remotely from each other. Groupware services can include the sharing of calendars, collective writing, e-mail handling, shared database access, electronic meetings with each person able to see and display information to others, and other activities.

Examples of groupware include Lotus Notes and Microsoft Exchange.

**helper applications**

In Netscape and other Web browsers, a helper application is a program that can handle a specific kind of file, which is indicated in the file transmission header by its MIME type or in storage by its file name extension. A few helper applications, such as those that handle HTML, GIF, and JPEG files, come with the browser. Additional ones can be downloaded and added to the browser by the user. Other than those that come with the browser, helper applications are usually run in a separate window (unlike plug-in applications which are integrated with the main browser program).

**IMAP (Internet Message Access Protocol)**

IMAP (Internet Message Access Protocol) is a standard protocol for receiving e-mail from your local server. IMAP is a client-server protocol in which e-mail is received and held for you by your Internet server. You (or your e-mail client) can read, search, and delete your mail from the server, but basically the mail is maintained for you on your server. An alternative protocol is POP3 (Post Office Protocol 3). With POP3, your mail is saved for you in your mail box on the server, but you and your e-mail client consciously download it to your computer and it is no longer maintained on the server. IMAP can be thought of as a remote file server. POP can be thought of as a "store-and-forward" service. POP and IMAP deal with the receiving of e-mail from your local server and are not to be confused with SMTP, a protocol for transferring e-mail between points on the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. A Client-server mail protocols FAQ is available that discusses both POP3 and IMAP and provides links to their RFC specifications.

**ISP (Internet or independent service provider)**

An ISP is a company that provides individuals and other companies access to the Internet. An ISP owns or rents the equipment required to have points-of-presence

on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their customers. Among the largest ISPs are UUNet, PSINet, and Netcom. ISPs also include regional providers such as New England's NEARNet and the San Francisco Bay area BARNet; they also include hundreds of local providers. In addition, Internet users can also get access through on-line service providers (OSPs) such as America Online and the large telecommunication companies such as AT&T and MCI. There is a definitive list of ISPs world-wide, including ones in your area, at http://www.thelist.com.

**interoperability**

Interoperability is the ability for programs made by different vendors to exchange information and work together. They achieve this by adhering to standards.

**MAPI (Messaging Application Programming Interface)**

Microsoft and other companies developed MAPI (pronounced "mappy") to enable Windows apps to communicate with a variety of Windows-based mail clients. But MAPI works on a more everyday level, too: so-called mail-aware applications can exchange both mail and data with others on a network. This is a Windows-only standard.

For example, if I use cc:Mail as my mail client, and I'm editing a document in Microsoft Word, I can go to the File menu and select Send to mail the document without having to go into cc:Mail itself. MAPI is the protocol that allows the two programs to communicate.

**POP3 (Post Office Protocol 3)**

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client-server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape browser.

Ê An alternative protocol is IMAP (Interactive Mail Access Protocol). With IMAP, you view your e-mail at the server as though it was on your client computer. E-mail can be kept on and searched at the server. POP can be thought of as a "store-and-forward" service. IMAP can be thought of as a remote file server. POP and IMAP deal with the receiving of e-mail and are not to be confused with SMTP, a protocol for transferring e-mail across the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. A Client-server mail protocols FAQ is available that discusses both POP3 and IMAP and provides links to their RFC specifications.

**proprietary**

1. In marketroid-speak, superior; implies a product imbued with exclusive magic by the unmatched brilliance of the company's own hardware or software designers.

2. In the language of hackers and users, inferior; implies a product not conforming to open-systems standards, and thus one that puts the customer at the mercy of a

vendor who can inflate service and upgrade charges after the initial sale has locked the customer in.

**protocol**

A set of formal rules describing how to transmit data, especially across a network. Low level protocols define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and correction of the bit stream. High level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, sequencing of messages etc.

The Internet is a heterogeneous collection of networked computers: they can't just throw data at each other any old way. The reason all these computers can communicate with each other (either by modem or other connection) is because they conform to protocols, such as TCP/IP, PPP, SLIP, and FTP.

**scalability**

In information technology and usually in its marketing, the word scalability seems to have two usages:

1. It is the capacity for a computer application or product (hardware or software) to continue to function well as it (or its context) is rescaled (typically, to a larger size, but possibly to a smaller size). The rescaling can be of the product itself (for example, a line of computer systems of different sizes in terms of storage, RAM, and so forth) or in the scalable object's movement to a new context (for example, a new operating system).

ÊÊ An example: John Young in his book Exploring IBM's New-Age Mainframes describes the RS/6000 SP operating system as one that delivers scalability ("the ability to retain performance levels when adding additional processors").

2. It is the capacity not only to function well in the rescaled situation, but to actually take full advantage of it. For example, an application program would be scalable if it could be moved from a smaller to a larger operating system and take full advantage of the larger operating system in terms of performance (user response time and so forth) and the larger number of users that could be handled.

3. In a truly scalable product, increase in size could be managed by distributing the load across multiple machines, rather than just buying bigger and bigger boxes.

**server**

No, it's not a synonym for "waitron." A server is a fancy name for a computer that's hooked up to a network (such as your office LAN, or the Internet) or a piece of software that helps that computer do its job. Servers send files across the network where your computer (the "client") receives and interprets them. Servers on the Internet are generally hooked up 24 hours a day, ready to serve your needs (pun very much intended).

A server exists with relation to one or more clients. Typically on the Internet, a larger computer is a server and a smaller computer (for example, a workstation) is a client. Specific to the Web, a Web server is the computer serving requested HTML pages or files. A Web client is the computer associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers.

**service provider**

If you're reading this, you likely already know of the Internet service provider, or ISP. It's the company that provides the gateway between you and the Internet. On-line services such as America Online and CompuServe are also touting their ability to provide Internet access. When you use AOL as a launching pad, that service is acting as your ISP. Many users, especially the more experienced ones, cut to the chase and go with an ISP that sticks to Internet-only access; for a monthly fee subscribers dial in to access the Internet -- letting the ISP handle the cost of buying and maintaining those expensive computers and leased lines.

**SMTP (Simple Mail Transfer Protocol)**

SMTP is the protocol used for sending e-mail across the Internet; IMAP and POP are protocols for reading e-mail. For your client to send a message, it uses SMTP to communicate with your server, and then your server uses SMTP to deliver it to the recipient's server.

**standards**

Standards may specify patented technologies, in which case standards-setting organizations (such as the IEEE) require companies owning such patents to file a letter of intent showing that they will license the technology for a reasonable fee. The fee is negotiated and paid directly between the patent owner and the manufacturer.

Companies owning patents that are specified in standards may be obligated to collect such royalties; otherwise, the patent could be declared invalid (since the company is not enforcing it). The royalty may be included as part of the cost of purchasing a crucial IC needed to implement the technology, and the IC manufacturer would pay the royalty (or could be the owner of the patent).

Obtaining standards documents is often the best way to verify details of a technology. While Internet-related standards (for example, all of the RFCs) are available at no cost over the Internet, most standards-setting organizations fund much of their work from standards' sales.

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

The method of routing information to and from a remote computer while on the Internet. TCP tells the network how to bundle the individual packets of data, and IP handles the routing to your address.

**terminal emulator**

A terminal emulator is any software that, when you run it on a PC, makes the PC resemble a mainframe dumb terminal. We don't mean any offense to mainframe terminals, they're called "dumb" because they aren't capable of doing any processing themselves. They only provide a gateway to use the mainframe's processing muscle. With terminal-emulator software, your PC looks and acts like a terminal (such as the DEC VT100 or VT200) to the central computer to which it's connected.

**thread**

A thread is a multi-part virtual conversation on a given topic. Threads can exist in Usenet newsgroups, in the forums of an on-line service, or in the form of a series of e-mails. Within a given topic -- say, "Washington lobbyists" -- several conversations, or threads, may be active at any given time, much like the separate,

simultaneous conversations at a cocktail party. In the case of Usenet and on-line service forums, generally the post which started the conversation (or fight, more often than not), is listed first, with responses from other participants following it, responding to either the original post or other's responses.

## APPENDIX B

## EMPLOYEE COVER LETTER

*We developed a cover letter for current staff to explain in writing why we are implementing a new policy. The current staff received this letter and the new policy. Once the policy was in place new employees only receive the policy.*

On Company letterhead

DATE: Current date

TO: All MAPS employees

FROM: Marsha Thiel, RN
Administrator

SUBJECT: Electronic Security and Monitoring Policy

MAPS made a considerable investment in computer hardware and software for the purpose of reaching our medical and business goals. In view of recent computer virus attacks and the potential for serious damage and misuse of our computer systems, it is imperative that our company develops and maintains a formal policy regarding the use of our information technology resources.

The following is our current policy:

Employees of MAPS are provided access to company telephones, voice-mail, computers, email, networks, internet systems, fax machines, equipment and other furnishings (including desks, drawers and cabinets) for the purpose of performing their job-related duties on behalf of MAPS.

Due to our need to protect our corporate assets from being used for improper purposes, MAPS has updated the policy. Each employee will be expected to understand and comply with the revised policy.

## APPENDIX C

## MAPS POLICY

(On company letterhead)

MEDICAL ADVANCED PAIN SPECIALISTS

ELECTRONIC SECURITY AND MONITORING POLICY

1. All MAPS employees who are entrusted with any company facilities or equipment, including but not limited to computer, email, network, Internet and voice-mail systems, are prohibited from using any such company assets for an improper purpose. Improper purpose includes but is not limited to sexual, racial or any other form of harassment against any employee, customer or any other person; pornography; personal use of any equipment which interferes with an employee's productivity and job performance; unauthorized disclosure of MAPS' confidential information; employee theft or violation of any law; solicitation of any kind; or any other use of MAPS computers or other equipment which is not related to MAPS business or which is deemed, in the sole discretion of MAPS, to be inappropriate and inconsistent with MAPS policies and corporate culture.

2. Email and Internet access is provided for MAPS business use only. Use for informal and/or personal purposes is permissible only within reasonable limits. All email and Internet records are considered company records and should be transmitted only to individuals who have business need to receive them. Those who have personal, confidential matters to communicate should, to assure privacy, not use company computers or equipment, including fax machines.

3. Additionally, MAPS email and Internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes. Consequently, you should always ensure that the business information contained in these messages is accurate, appropriate and lawful.

4. MAPS reserves the right of immediate access to any company equipment, including all information stored on any MAPS computer or phone system, upon reasonable concern that the employee entrusted with such equipment is using it for an improper purpose. MAPS also reserves the right to conduct random reviews of employees' computers, email and voice-mail systems for the purpose of ensuring that this equipment is being used for the business purposes for which they are intended and not for any improper purpose.

5. Consistent with the above, MAPS employees may not expect or assert a right of privacy in connection with any company-owned assets. Email and voicemail messages and Internet records are to be treated like shared paper files, with the

expectation that anything in them is available for review by authorized MAPS representatives.

6. MAPS reserves the right to monitor employees' incoming and outgoing phone calls on our business phone lines on a random basis for training, quality assurance, customer service and disciplinary purposes to determine whether excess personal phone calls are occurring during business hours. If monitoring occurs and the company representative determines that the phone call is personal, he or she will immediately hang up the phone. Personal phone calls on company time are prohibited, except in case of emergency. Employees may make personal calls during breaks and other non-work time.

7. Each employee's computer password and any other confidential access code must be on file with their immediate supervisor and system administrator.

8. Employees are prohibited from accessing other employees' email and voice-mail files and computers, except as specifically authorized by their supervisors in connection with their work for MAPS.

9. Providing any non-authorized MAPS employee or any non-employee with access information or permitting such persons the use of MAPS computer equipment is prohibited.

10. Entering information into a computer or database that is known to be false and/or unauthorized, or altering an existing database, document or computer disk with false and/or unauthorized information is prohibited.

11. Making any modification to MAPS computer equipment, systems files or software without specific authorization is prohibited. Modification includes the installation of any software on any MAPS equipment.

12. Computer equipment, systems files or software programs may not be removed from MAPS, reproduced, or used in any way to duplicate software, unless specifically authorized by the Systems Administrator.

13. Any announcement, which any employee wishes to make over our email system that is not strictly related to company business must be approved in advance by the department manager and must be of general interest to MAPS employees.

14. Employees' communications on MAPS electronic systems should be cordial, professional and inoffensive to individuals or groups. If in doubt, leave it out. Examples of prohibited communications include sexual, racial, ethnic, and religious comments or portrayals; perceived slurs on the character of individuals or groups; stances on political issues or other topics that could cause controversy either within or outside MAPS. Also, since we are using our electronic

communication systems in a professional place of business, no attempt should be made to influence the personal values or beliefs of others.

Employee Signature: _____ Date: _____

Manager: _____ Date: _____

## APPENDIX D

## ACRONYMS and EMOTICONS

| | |
|---|---|
| BTW | By the way |
| FAQ | Frequently asked questions |
| FYI | For your information |
| FWIW | For what it is worth |
| IMHO | In my honest/humble opinion |
| JTYLTK | Just thought you'd like to know |
| LOL | Laughing out loud |
| OTOH | On the other hand |
| PLS | Please |
| RFC | Request for comments |
| RTM | Read the manual |
| TIA | Thanks in advance |
| TNX | Thanks |
| TTYL | Talk to you later |

| | |
|---|---|
| :-) | Sender is happy (or message is positive) |
| :-( | Sender is sad (or message is negative) |
| B-) | Sender wears glasses |
| ;-) | Sender is winking |