

CURRENT PRACTICES IN ELECTRONIC COMMUNICATION MANAGEMENT

Richard Glass, PhD, Bryant University, rclass@bryant.edu
Nancy Records, MS,MBA, Bryant University, nrecords@bryant.edu
Hal Records, PhD, Bryant University, hrecords@bryant.edu
Robert Behling, PhD, Arrowrock Industries, behlingr@hotmail.com

ABSTRACT

Virtually all corporations use e-mail as a method of electronic communication in their organizations. Yet many organizations report that their e-mail management systems are in "complete chaos." Instant messaging (IM) is a rapidly emerging electronic communication technology that is already being used for business applications by 60% of mid to large enterprises. Both Ostermann Research and Gartner project that the adoption rate of IM in business will approach 100% by 2010. In one survey conducted by AIIM, more than 70% of organizations reported that they did not have formal policies for instant messaging. This paper describes the results of a detailed survey of management practices for e-mail and instant messaging among organizations in the Northeast United States. Findings support earlier studies that despite 100% acceptance and use of e-mail among organizations, e-mail management practices are often lacking in corporations. Similar to the 2005 AIIM study, IM was allowed to be used for business purposes by 45% of organizations surveyed. Management practices for IM were found to be in a lesser state of development than e-mail management practices. Results of the survey are reported in this paper and implications for organizations are discussed.

Keywords: electronic communication management, e-mail, instant messaging, electronic communication security, electronic communication policies.

INTRODUCTION

With the proliferation of desktop computing in every business environment, employees at all levels within an organization have access to very seductive technologies. Among the most popular and easiest to use are e-mail and instant messaging. Virtually all enterprises use e-mail for business purposes [3]. E-mail is used in business more frequently than telephone, fax or physical correspondence and as much as 60% of business critical information is contained in e-mail [18]. E-mail is now considered to be a mission critical application for organizations

and the reliance on e-mail to conduct business is likely to grow given that e-mail use is predicted to increase by 40 percent a year over the next several years [11].

Instant messaging (IM) is an emerging communication technology that allows employees to send and receive short text-based messages in real-time and to see who else is online and currently available to receive messages [6]. IM is rapidly growing in popularity within business. Giga Information Group reports that 60% of mid to large enterprises have some level of IM being used for business application [14]. A Computerworld survey of 113 IT managers found that 40 percent use IM as a sanctioned form of interoffice or intercompany communication [2]. Both Gartner and Osterman Research project that the adoption rate of IM in business will approach 100% by 2010.

The allure of electronic communication in an organization may be attributed in large part to the growth of telecommuting and the emergence of virtual organizations. Facetime Communications [9] reports that research data indicates that 1) 58% of IT executives consider their company to be a virtual workplace, 2) 75% IT executives regularly use real-time communications technologies, 3) 60-70% of employees work in different locations than their managers and 4) 90% of employees work in locations other than corporate headquarters.

E-mail first became a popular business tool during the 1990's. However, after nearly two decades of use in corporations, organizations are still preoccupied with productivity issues, exposure and risk to the business and the legal issues that are associated with electronic communication. IM is a relatively new technology and has received considerably less attention by management. An Association for Information and Image Management (AIIM) study of US organizations found that 48% of firms allow their employees to use IM for business purposes. However, only 28% had formal policies regarding the use of IM [3].

The purpose of this study is to investigate whether organizations in the Northeast United States have implemented workplace e-mail and instant messaging management policies. Implications of the findings are discussed and recommendations are provided for implementing electronic messaging management policies in organizations.

ELECTRONIC COMMUNICATION MANAGEMENT

Wilkins [17] suggests that organizations move through four phases of new technology adoption; Ignorance, Denial, Acceptance and Optimization. During the Ignorance phase the organization does not know about the technology and does not believe that their employees know about the technology. In the Denial phase, the organization recognizes that the technology is present and forbids its use for several productivity and security reasons. With time, the organization enters into the Acceptance phase wherein the organization officially recognizes the technology and undertakes efforts to control the use of the technology in the organization. During the final, Optimization phase the technology is integrated into existing business processes and optimized. In this phase the technology is considered to be a mission critical application. Wilkins suggests that e-mail is currently a mission critical application and that it is in the Optimization phase in many organizations. He suggests that IM is only now emerging as a supported technology and organization are just beginning to enter into the Acceptance stage.

There are several references to e-mail being a mission critical application in the literature. Julien [11] considers e-mail to be a mission critical application given that e-mail is the primary form of communication for the exchange of thoughts, ideas and information in an organization. Mancini [12] points out that e-mail is the central means by which most business decisions are documented. Winkler [18] claims that e-mail is mission critical and is more important than many other IT applications and systems. Industry statistics clearly demonstrate that e-mail is an accepted technology in virtually all business organizations with 99% of business employees using e-mail and 83% of organization having implemented an e-mail policy [3].

These statements would lead one to believe that e-mail is well entrenched in the Optimization stage of technology adoption. A more detailed look at how e-mail is being managed in organizations provides a much different picture. A recent survey in the UK [2] found that 38% of large organizations admitted that

their e-mail management systems were in "complete chaos." In a survey that included the world's 14 largest banks, health care firms, manufacturers and small business, Marshall found that 48% of the firms allow total access to personal e-mail accounts while on the job [8]. Mancini [12] suggests that most organizations continue to have a very casual attitude towards e-mail management. He reports that 35% of end users indicated that they have not yet begun to address such core e-mail management issues as archiving, life cycle management, retention and disposition. Another 41% have begun to address e-mail management but state that much remains to be done. He further suggests that most organizations leave the management of e-mail up to the individual employees with 62% of respondents surveyed indicating that there is no definition of e-mail management in their organization. In a study of workplace e-mail conducted by the American Management Association [5] it was found that: 1) 46% of responding companies offer no e-mail policy training to their employees; 2) 65% of responding companies lack e-mail retention policies; 3) 13% of responding companies have had lawsuits triggered by employee e-mail; 4) 21% of responding companies have had employee e-mail subpoenaed in the course of a lawsuit; 5) 25% of responding companies have terminated an employee for violating e-mail policies; and 6) 50% of the workplace instant messaging users send or receive risky content.

In spite of a virtual 100% acceptance rate in organizations, it appears that many firms still lack comprehensive formal management policies to take control of e-mail technology and are still entrenched in the Acceptance stage. Given the results of the above surveys, it would be premature to claim that e-mail technology is in the Optimization stage of adoption.

IM is currently in transition from the Denial stage to the Acceptance stage. A 2005 AIIM study [3] found that 48% of businesses permit the use of IM for business purposes. It is expected that 100% of businesses will permit the use of IM for business purposes by 2010 [18]. The Radicanti Group [7] estimates that the business IM market will grow from an installed base of 65 million in 2007 to 127 Million in 2011. Yet several organizations still ban the use of IM altogether [16]. Of those companies that permit the use of IM in the organization, IM management policies are ill formed or nonexistent. AIIM found that only 28% of firms studied employed formal IM policies. Of the firms that have IM management policies about two thirds allow their employees to use unprotected IM services such as AOL, AIM and

Microsoft MSN [13, 16]. Some 58% of IM users regularly engage in personal chat at work [10]. Giga Information Group reports that 90% of the

The results of the surveys cited above suggest that there are serious gaps in the management of electronic messaging within many organizations. The gaps exist for both more mature e-mail technology and emerging IM technology. Several of the survey results however, are more than two years old. To gain a more current perspective the authors developed a survey instrument to investigate whether organizations in the Northeast United States have implemented workplace e-mail and IM management policies.

METHODOLOGY

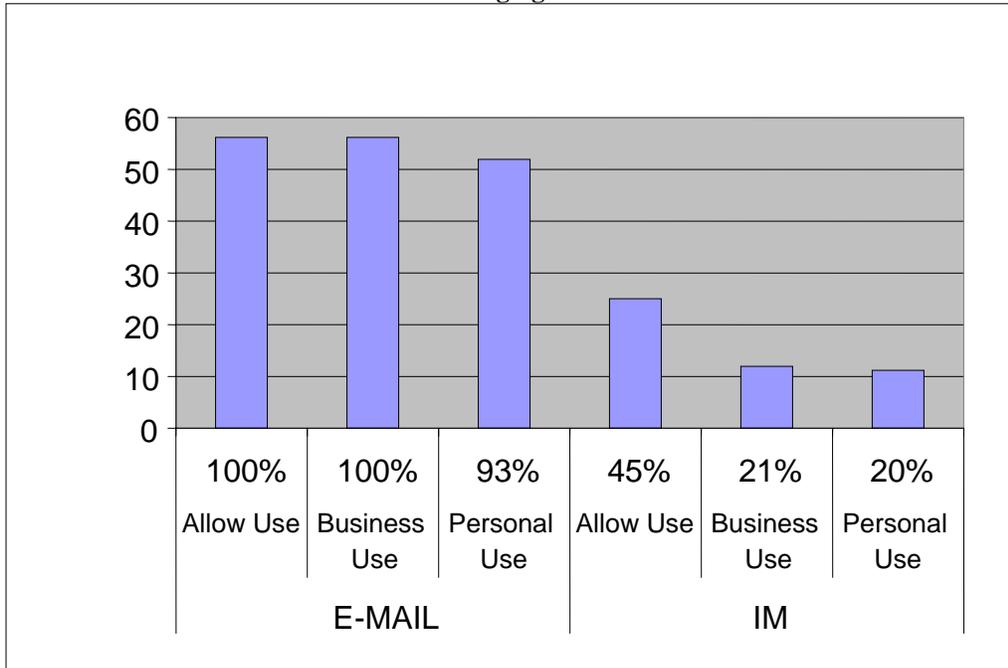
An electronic communication technology survey was administered to 64 MBA students enrolled in a Northeast university. Two respondents were eliminated because they were not employed at the time the survey was administered and six respondents were eliminated because of duplication in the organizations in which they worked. The total number of respondents included in the analysis is 56, representing 41 different firms. While the survey population is not representative of a cross section of

organizations using IM have no formal IT support and less than 10% have implemented secure, enterprise IM [14]. the American workforce, these graduate students are business professionals who are, or may soon be senior managers. Firms were categorized as Service (80% of respondents) or Manufacturing (20% of respondents). Of firms represented by the respondents 9% were one to fifty employees, 21% fifty one to five hundred, 25% five hundred one to two thousand, 15% two thousand one to ten thousand, and 30% greater than ten thousand.

FINDINGS

Consistent with past findings, e-mail is allowed for business use by virtually all firms in the survey and 100% of respondents use it for business. Practically all respondents (93%) use email for personal use while on the job. Instant messaging (IM) is allowed by 45% of firms being reported. This result is approximately the same as the 2005 AIIM survey which reported 48%. With respect to use, 21% use it for business and 20% for personal purposes which suggests that as IM penetration into businesses grows, its utilization will be similar to e-mail in that it will be used for both business and personal purposes.

Exhibit 1: Use of E-Mail and Instant Messaging



E-mail remains the predominant means of electronic communication in business both in numbers of daily communications and percentage of time spent, but

table 1 shows that IM is beginning to have a presence in the organization.

Table 1: Comparison of e-Mail and IM Usage

Received per Day	e-Mail	IM	% of Day Spent	e-Mail	IM
None	0%	68%	< 10%	25%	93%
1 to 20	39%	14%	10% to 20%	30%	7%
21 to 40	18%	4%	21% to 30%	21%	0%
41 to 60	14%	4%	31% to 40%	4%	0%
61 to 80	9%	0%	40% to 50%	13%	0%
81 to 100	5%	0%	>50%	5%	0%
> 100	13%	5%			

When asked whether their organization has a formal e-mail technology in place, 40 respondents (70%) responded positively, 8 (15%) answered no and 8 (15%) did not know. The AIIM study found that 83% of firms had a formal e-mail policy. Given that 15% did not know, it is difficult to compare the two studies, however the results do indicate that a large percentage (30%) of respondents either did not have a formal e-mail policy or were not aware that one existed. Of the 25 respondents who indicated that their firms permitted the use of IM only 5 (20%) indicated that their organization had a formal policy with 11 (44%) reporting that they had no formal policy and 9 (36%) indicating that they did not know. The AIIM study found that 28% had formal IM policies.

content of the policies was incomplete. All 40 respondents who reported formal e-mail policies indicated that their organization had an acceptable use policy as did all 5 respondents who reported formal IM policies. The results for policy attributes indicate much lower response rates with corresponding increases in those who responded that they did not know. Respondents generally found e-mail policies clearly written, easy to understand and easy to comply with. More respondents did however, report e-mail policies to be difficult to access and often not reviewed or updated. Many respondents did not know whether e-mail policies were reviewed and updated by their organizations. As shown by Table 2, Instant Messaging Policy Attributes are rated as being much less mature than those of e-mail.

Even when respondents indicated that their organization had formal policies for e-mail or IM, the

Table 2: Electronic Communication Policy Attributes

Characteristic	e-Mail			IM		
	Yes	No	Do not Know	Yes	No	Do not Know
Easy to Access	46%	18%	29%	9%	23%	41%
Clearly Written	55%	13%	25%	11%	21%	43%
Easy to Understand	59%	9%	25%	9%	21%	43%
Easy to Comply	61%	7%	27%	11%	21%	41%
Reviewed and Updated	38%	13%	41%	7%	21%	43%

% add up to less than 100% because not all respondents answered

The enforcement of electronic communication policies is critical to the effective use of the technology in the organization [11]. According to respondents of those firms having an electronic communication policy, 41% included a use-monitoring scheme, 46% a list of banned activities,

21% remedies for inappropriate behavior, and 20% contained enforcement consequences. Table 3 summarizes these results.

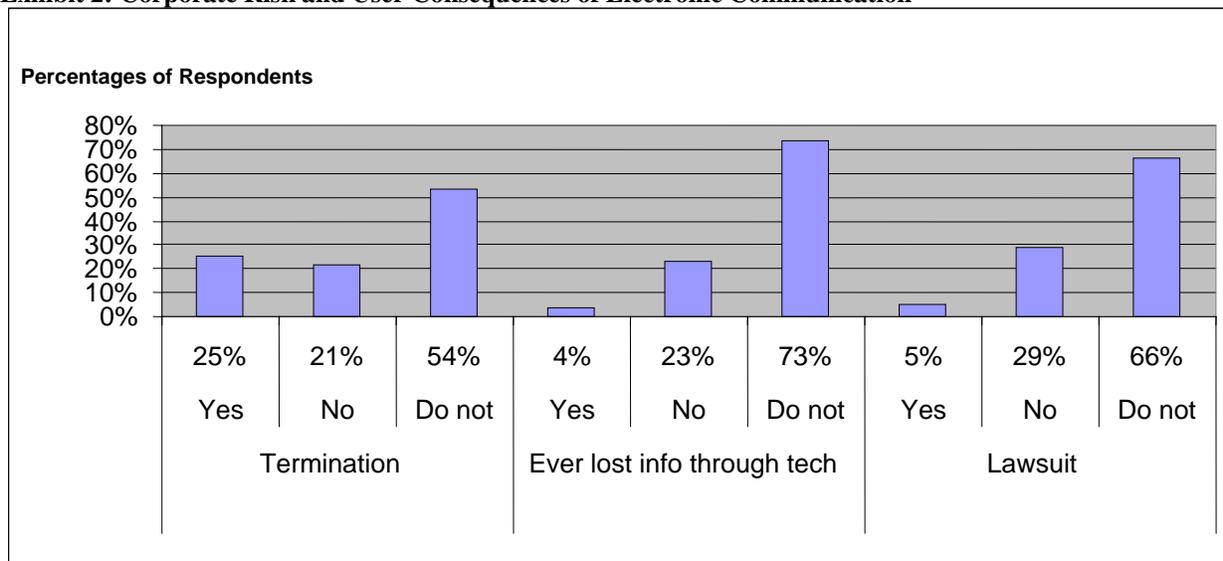
Table 3: Enforcement Policies

Type of Enforcement Policy	Percent of Respondents
No Policy	9%
Monitoring Scheme	41%
Banned Activities	46%
Remedies for Inappropriate Behavior	21%
Policy not Enforced	20%
Other	7%

As shown by Exhibit 2 – Corporate Risk and User Consequences of Electronic Communication, 4% of firms experienced lost information and 5% encountered a lawsuit. On the consequence side 25% of respondents indicated knowledge of a termination resulting from improper use of electronic

communication. This suggests that in the interest of prevention, management strives to make consequences to employees widely known while making instances of IT related information breaches and legal actions less so.

Exhibit 2: Corporate Risk and User Consequences of Electronic Communication



Train [15] suggests that it is unfair to publish an electronic communication policy without ensuring that the employees are fully trained and aware of the policy. All organizations employ e-mail for business purposes but only 71% of respondents indicated that they had some e-mail training. Of the respondents whose organizations permit IM for business purposes, only 18% had some training.

CONCLUSION

This survey indicates that there has been little improvement in organizations’ management of e-mail and IM communication technologies over the last few years. IM has not increased in sanctioned use by organizations since the AIIM 2005 survey and the implementation of formal management policies to control both IM and e-mail is sadly lacking. These results are particularly troubling in light of the fact that the volume of e-mail and IM in organizations is

increasing at exponential rates bringing with it an increasing array of spam, viruses and security exploits [4]. Retention policies for e-mail and IM are also seriously lacking given the post 9/11 requirements for compliance. One survey reported that 60% of users failed to acknowledge that e-mail falls under the compliance requirements for enterprise content management [2].

If one considers the results of this survey with the recommendations of the epolicyinstitute listed below, it is apparent that companies are deficient in all areas. The epolicyinstitute recommendations include [5]:

1. Make policy development, training and monitoring a company wide priority
2. Prepare a policy manual for distribution to all employees, and establish a mandatory training program that describes the risks,

- defines the policies, and discusses monitoring employee internet use.
3. Establish and make public rules for personal internet use.
 4. Develop, make public and implement a plan for comprehensive monitoring of employee internet activity.
 5. Review monitoring procedures with all employees and clearly describe disciplinary actions to be expected when policies are violated.
 6. Have employees sign a statement that they know and understand the internet policies.
 7. Enforce policies, especially content rules. E-mail creates a written business record that is admissible in court.

IMPLICATIONS FOR FUTURE RESEARCH

Electronic communication is such a pervasive and growing phenomena in business, and because it presents such significant risks and opportunities further research should be conducted at regular intervals to see if IM does in fact move from a denial to an acceptance phase, to see if IM is becoming as pervasive as e-mail, and to see if firms are doing a better job of implementing and enforcing electronic communication policies. The results of this survey are consistent with prior survey findings that indicate serious failings in current practices in electronic communication management. Case studies of organizations that have implemented best practices should be undertaken to identify the organizational factors that have contributed to successful electronic communication practices and guidelines developed to help organizations improve their management practices.

REFERENCES

1. _____. (2007) Best Practices to Minimize Risk. Found at: www.epolicyinstitute.com
2. _____. (2007) Companies Admit to Email Management System Chaos. Business News, found at www.instam.org.
3. _____. (2005) Electronic Communication Policies and Procedures: a 2005 Industry Study. Found at www.aiim.org.
4. _____. (2005) Email Management, Datamonitor, August, 2005. Found at: www.datamonitor.com.
5. AMA. (2004) American Management Association 2004 E-Mail Survey. Found at: www.epolicyinstitute.com/survey.index.html.
6. Cameron, A. F. and Webster, J. (2005). Unintended Consequences of Emerging Communication Technologies: Instant Messaging in the Workplace. *Computers in Human Behavior*, January 2005, 85-103.
7. Dubie, D. (2007) Fantasy Football, IM throwing productivity for a Loss, *Network World*, found at www.networkworld.com/news/2007/112607.
8. Gibson, P. (2006) Personal Email Use at Work Creates Big Security Risks. *Bank Technology*, December 2006, 21.
9. Facetime Communication Inc. (2005) Securing Unified Communications: From Consumer-Based IM to Enterprise Collaboration and Beyond. Found at www.facetime.com.
10. IMIN (2006) The Harm Instant Messaging Can Do to Your Business: Business Solutions for Secure Instant Messaging. Found at www.EBS-IMIN.com.
11. Julien, J. (2007) Championing Email Management. *Edocmagazine*, found at www.edocmagazine.com.
12. Mancini, J. (2006) Email Management. *Edocmagazine*, found at www.edocmagazine.com.
13. MessageLabs (2007) Instant Messaging: Benefits and Threats for Business. Found at www.messagelabs.com.
14. Secure Computing (2006) Benefits of Enterprise Instant Messaging. Found at www.securecomputing.com.
15. Train, T. K. (2006) Email Management Compliance. *Edocmagazine*, found at www.edocmagazine.com.
16. Turek M. (2006) Instant Messaging: Security, Control and Compliance. *Business Communications Review*, June 2006, 32-36.
17. Wilkins, J. (2007) RU Ready For IM? *The Information Management Journal*, May/June 2007, 27-31.
18. Winkler, D. (2005) E-Mail Management: Compliance, Control, Consolidation. *Computer Technology Review*, 25(2), 12-13.