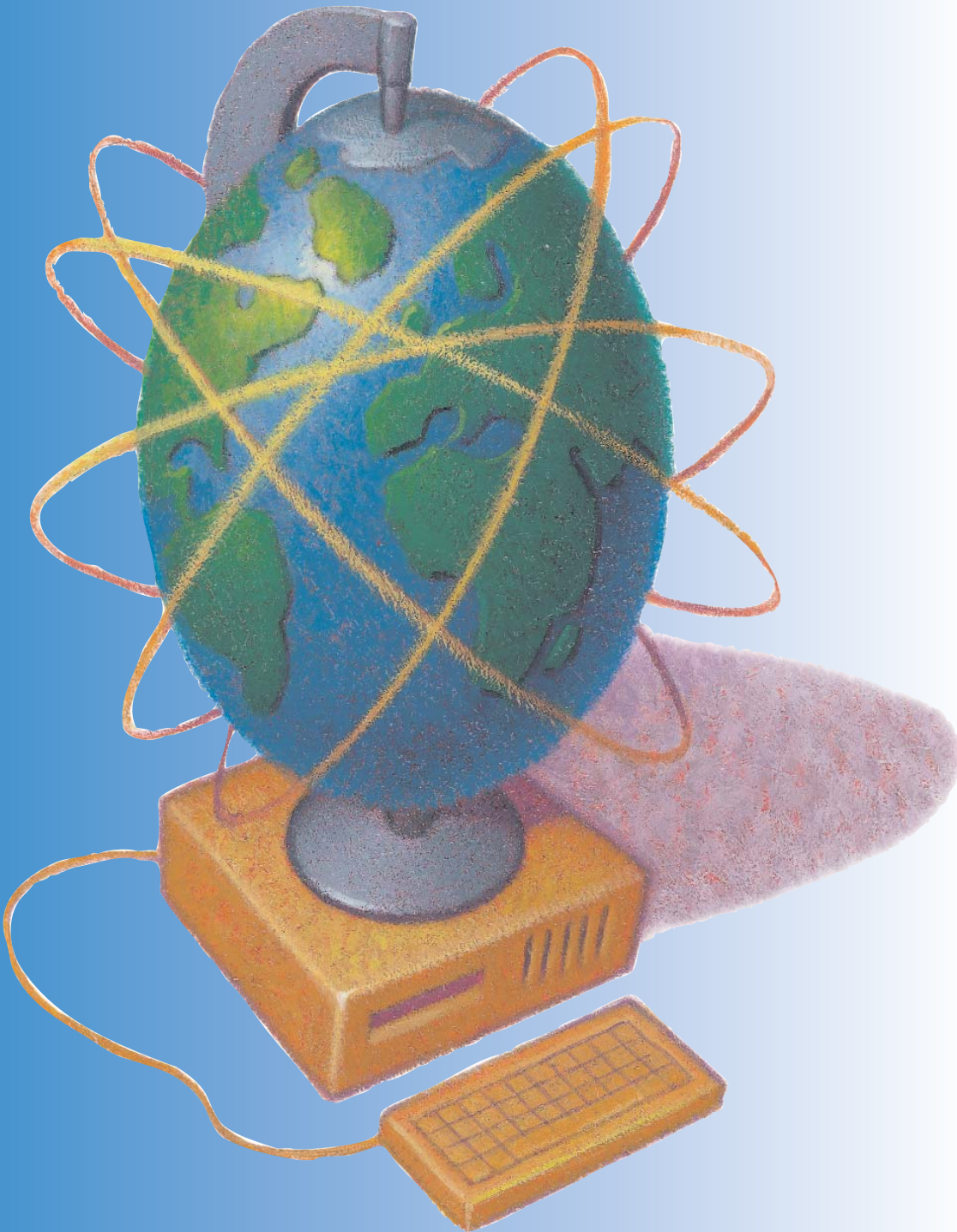


# *2004 E-Mail Survey*

*LawNet's Third Annual Report on E-Mail Usage  
and Administration*

August 2004



A Publication of LawNet, Inc.

## About LawNet

---

Providing technology solutions to law firms and legal departments gets more complex every day. Connecting with your peers to exchange ideas with those who have “been there, done that” has never been more valuable.

For over two decades, LawNet has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. LawNet members come from firms of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

*LawNet's Statement of Purpose: LawNet is the premier peer networking organization providing information resources to members in order to make technology work for the legal profession.*

## Editors' Note

---

Commend it or condemn it — and who among us doesn't routinely do both! — e-mail is as much a part of our work lives as our paychecks. So arguably, as one of the markets that uses and depends on it the most, it behooves us to stay as informed about the challenges, solutions and trends in e-mail management as we possibly can. This makes our 2004 E-Mail Survey, LawNet's third, as timely and useful as any survey or white paper we publish. This year's e-mail survey responses represent 378 organizations employing close to 60,000 attorneys — and we thank you all for your participation.

We want to specifically acknowledge **Todd Corham**, Director of Information Technology at Lowenstein Sandler PC, whose commitment to this on-going survey over three years, to say nothing of the time and analytical detail that he devotes to the project each year, is to be applauded.

*Andy Spiegel and Randi Mayes, Editors*

---

## Table of Contents

LawNet's 2004 E-Mail Survey Results (Narrative Analysis) .....	3
<i>by Todd Corham of Lowenstein Sandler PC</i>	
2004 Survey Data .....	5
The Shifting Tactics of Spammers .....	10
<i>by Andrew Lochart of Postini, Inc.</i>	
E-Mail Management: The New Imperative .....	12
<i>by Neil Araujo of Interwoven</i>	
CRM to Manage E-Mail .....	13
<i>by Barry Solomon of Interface Software</i>	
Website Content Management System .....	14
<i>by Sonny Cohen of Duo Consulting</i>	

---

### Disclaimer

This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither LawNet, Inc. nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

LawNet, Inc., a U.S.-based association, has no connection or affiliation with LawNet Ltd., which is a group of independent law firms operating throughout the United Kingdom and the Republic of Ireland. In the United Kingdom, LawNet, Inc. will be referenced as peertopeer.org. We regret any inconvenience that may have arisen as a result of the use of the name “LawNet, Inc.” in the United Kingdom.

---

### Copyright Notice

Copyright © LawNet, Inc. 2004. All rights reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of LawNet, Inc. Published by LawNet, Inc. c/o Andy Spiegel, 2110 Slaughter Lane, #115, PMB 149, Austin, TX 78748.



# LawNet's 2004 E-Mail Survey Results

by Todd Corham of Lowenstein Sandler PC



The LawNet team, including the many LawNet members who took the time (from managing e-mail, perhaps?) to contribute their experiences to this survey, has pulled together a pool of data aimed at revealing practices and trends in the increasingly challenging management of e-mail at law firms and legal departments. This being the third annual survey, it's actually the first time we were able to spot some trends in e-mail use and practices. A great deal of time was spent reviewing and analyzing the responses; and though we did our best to arrive at some conclusions in this report, we strongly encourage you to study the compiled answers and impose your own interpretations before making significant decisions regarding your e-mail system and its management.

This year's response represents 378 organizations employing close to 60,000 attorneys. Since recipients continue to observe that grouping responses by the size of the organization is useful in interpreting and employing the data, we've included many charts arranged by size. 85 firms represent 200 attorneys and above, 189 firms and law departments report 50 to 199 attorneys, and 102 organizations were fewer than 50 attorneys (two respondents did not report a size.)

## E-Mail: A Continuing Challenge

It's obvious from the data that e-mail administrators are being squeezed by opposing forces that demand conflicting policies on e-mail retention. Attorneys are increasingly relying on e-mail as the backbone of their practice and therefore are more insistent that it not be deleted and that access to e-mail history be as close to unlimited as possible. On the other side, mailbox files are bursting at the seams, threatening the stability and availability of the e-mail platform.

*The best evidence of user resistance is how fast the average size of mailbox limits has increased. The average limit went from 200MB in 2003 to 350MB this year — a 75% jump. In fact, the limitation of mailbox sizes as a practice is actually down 8% over the last two years, and many respondents commented that even these limits are somewhat “flexible.” Imposing restrictions on mailbox size by job description, however, is up 5% over 2002, so it appears that administrators will take whatever relief they can get.*

*It is 6% more common now than two years ago to back up the e-mail system (all but 2% do so), even if the tapes are kept only for a short period of time (81% overwrite them.) The policy of total destruction of e-mail files is essentially flat from last year (down a statistically irrelevant 1%) and is practiced by 8% of firms that responded. It is interesting to note that 10% of firms have a “destruction policy,” but most of them have not been able to prevent the practice of archiving. Again, the pressure from attorneys for access to e-mail history is increasingly difficult to withstand.*

*E-mail administrators, looking perhaps for other methods of controlling the flood, are putting restrictions on the size of e-mail transmissions at a greater rate than previous years. The practice of using incoming size limits are up 8% since 2002, and for outgoing mail the practice has increased 9% during that same period.*

*Instant Messaging is undoubtedly growing industry-wide, but more firms are taking a stand against it this year. Nevertheless, the number of firms in which IM is used regardless of policy has stayed constant from last year. This may reflect the fact that IM use is quickly becoming part of the culture, and those who were not able to draw the line early face an uphill battle at this stage.*

## The Hunt for Solutions Goes On

So how are we dealing with e-mail history? Larger firms are more likely to “age” the mail in the users’ mailboxes (56% of larger firms report that policy, as opposed to 27% and 19% for medium and small organizations, respectively.) That could mean that the larger firms are relying on archiving (they are archiving slightly more than their smaller counterparts,) or, as evidenced, are turning to third-party e-mail management systems, a practice large firms are 12% more likely to follow. Moving e-mail to an e-mail management application, as mentioned above, more than doubled since last year (17% to 37%) — this, at a time when the “process” is still evolving. We are in a transition period during which the practice of “e-mail history management” is migrating toward records management. The specific methods by which an attorney (1) “declares” an e-mail (or attachment) a “record” of the firm’s business, (2) moves it off the e-mail system, (3) subsequently references that record and then ultimately (4) subjects it to the firm’s stated “lifecycle policies” have yet to be fully worked out. But that has not deterred some firms from getting the process started (most commonly with iManage and Hummingbird), even if the tools for facilitating the process are not yet in place.

## Arming for Battle

Along with the new e-mail management functionality our members are exploring, new strategies are also emerging for the other challenges we face:

***Anti-Virus** — Almost three quarters of respondents now employ a second virus scanner (up 27% over last year), yet one in five of those firms with double scanning still reported downtime due to virus attacks. 38 unique solutions for the anti-virus effort were reported by our users.*

***Anti-Spam** — It is probably no surprise that Postini has become the spam filter of choice, capturing 35% of the market in just one year (up from 10 installations.) If Postini does not have the spam-fighting model you prefer, there are 57 other anti-spam packages in use by our members.*

***Quarantine Management** — Allowing users to manage their own quarantine logs is an option growing in popularity at many organizations. 60% of firms now ask users to do their own quarantine monitoring, relieving the IT department of the burden.*

Even with the above assistance, 46% of respondents report spending “more” or “significantly more” time managing issues related to e-mail. Those firms that reported spending “less” or “significantly less” time were unique in a few categories:

almost all have two virus scanners; few reported suffering downtime from viruses; and they are much more likely (statistically) to allow users to handle quarantine logs.

## Looking to the Future

Not to make too much of apparent trends with only a few years of data behind us, but there are some areas of the e-mail challenge that are moving in a perceptible direction:

*We can expect vendors to deliver increasingly sophisticated methods of moving e-mail into management applications off the e-mail server. The need has been clearly evident for several years, and the solutions will begin to appear in both first- and second-generation solutions in the year ahead.*

*We will probably see increasing convergence between the records management and document management worlds — the bellwether being Hummingbird’s acquisition of LegalKEY.*

*Our ability to put restrictions on mailbox sizes and on e-mail file sizes, as well as to “age” mail, will increase only when we find some other place to put the history, making it accessible and searchable in full text. The practice of allowing users to archive to the C: drive will begin to haunt us as PCs crash, subpoenas for that data appear and users become more mobile.*

*As the focus on e-mail-borne viruses solidifies, our virus exposure will begin to shift to Web-browsing (personal e-mail accounts) and Instant Messaging. The window will be small (during those few hours following the outbreak and before we can download the new definition file to the desktop) but nonetheless dangerous.*

## Closing Thoughts

Not all aspects of e-mail use were polled, and yet the sheer number of data points in this survey gives an indication of how many decisions there are to be made in the course of administering an e-mail environment. Each decision we make impacts others, and these cascade into an interdependent pattern that is a reflection of our firm culture and user requirements.

We hope this survey will be of assistance as you make those decisions. The data in these surveys becomes increasingly useful, accurate and actionable as the participation increases, so to everyone who took the time to respond to our questionnaire, we extend our gratitude and appreciation.

One last thing reminder: please turn off e-mail notifications to senders of incoming viruses. They rarely contain legitimate return addresses, and they just serve to confuse users and clutter the landscape.

## 2004 Survey Data

	All Firms Combined	200 Attys & Over	Firms 50 to 199 Attys	Firms under 50 Attys
1. What is your e-mail platform?: (Last year - Exchange 71%, GroupWise 22%, Notes 5%)	Exchange 301 (80%) GroupWise 59 (16%) Notes 15 (4%) Other 3 (<1%)	Exchange 68 (80%) GroupWise 10 (12%) Notes 7 (8%) Other 0 (0%)	Exchange 154 (81%) GroupWise 28 (15%) Notes 5 (3%) Other 2 (1%)	Exchange 79 (76%) GroupWise 21 (20%) Notes 3 (3%) Other 1 (1%)
2. Does your firm offer Web access to e-mail? ("Yes" responses were up 7% over last year)	Yes 338 (90%) No 39 (10%)	Yes 80 (95%) No 4 (5%)	Yes 173 (92%) No 16 (8%)	Yes 85 (82%) No 19 (18%)
3. Do you set a limit on mailbox size? (Last year - Yes 30%, No 70%)	Yes 108 (29%) No 267 (71%)	Yes 23 (27%) No 61 (73%)	Yes 56 (30%) No 132 (70%)	Yes 29 (28%) No 74 (72%)
4. If so, what is that limit? As in prior years, the most often cited limit is 100MB (17 firms out of 100 respondents.) 60% of respondents reported limits from 100MB to 500MB. The other 40% ranged from a low of 300KB (!) to a high of 2GB.				
5. Do you restrict mailbox size by job function? (Last year - 11% Yes, 89% No)	Yes 49 (13%) No 325 (87%)	Yes 13 (16%) No 70 (84%)	Yes 26 (14%) No 162 (86%)	Yes 10 (10%) No 93 (90%)
6. Does your firm routinely back up the e-mail system? (Last year - 95% Yes, 5% No)	Yes 369 (98%) No 9 (2%)	Yes 82 (96%) No 3 (4%)	Yes 184 (97%) No 5 (3%)	Yes 103 (99%) No 1 (1%)
7. If so, do you routinely overwrite tapes (preventing a long-term e-mail record)? (Last year - 81% Yes, 19% No)	Yes 302 (81%) No 70 (19%)	Yes 63 (76%) No 20 (24%)	Yes 152 (82%) No 34 (18%)	Yes 87 (84%) No 16 (16%)
8. Does the firm archive mail (or allow users to do so)? (Last year - 73% Yes, 27% No)	Yes 272 (72%) No 104 (28%)	Yes 63 (74%) No 22 (26%)	Yes 133 (71%) No 54 (29%)	Yes 76 (73%) No 28 (27%)
9. Does the firm "age" mail (delete mail after a designated period of time)? (Last year - 33% Yes, 67% No)	Yes 115 (31%) No 261 (69%)	Yes 45 (53%) No 40 (47%)	Yes 50 (27%) No 138 (73%)	Yes 20 (19%) No 83 (81%)
10. Does the firm have a stated e-mail "destruction" policy (all must be deleted after a specified period of time)? (Last year - 12% Yes, 88% No)	Yes 37 (10%) No 336 (90%)	Yes 12 (14%) No 72 (86%)	Yes 18 (10%) No 169 (90%)	Yes 7 (7%) No 95 (95%)

**All Firms Combined**

**200 Attys & Over**

**Firms 50 to 199 Attys**

**Firms under 50 Attys**

11. Do you use an e-mail management application (other than the native mailboxes in your mail program) to store and organize e-mail history? (Last year - 17% Yes, 83% No)

Yes	139	(37%)
No	237	(63%)

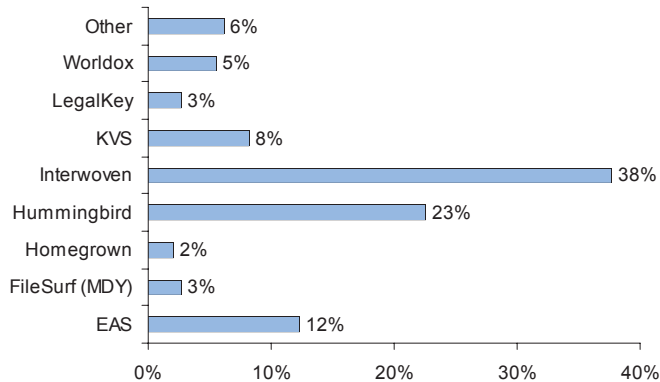
Yes	39	(46%)
No	45	(54%)

Yes	73	(39%)
No	116	(61%)

Yes	27	(26%)
No	76	(74%)

12. If so, which application do you use for e-mail management? (146 Responses, up 160% from last year)

**E-Mail Management Applications**



13. Does your firm limit the size of incoming mail? (Last year - 39% Yes, 61% No)

Yes	165	(44%)
No	207	(56%)

Yes	45	(53%)
No	40	(47%)

Yes	87	(47%)
No	97	(53%)

Yes	33	(32%)
No	70	(68%)

14. If yes, to what size do you limit incoming mail?

Of the 157 firms who listed an actual size limit, 22% reported 10MB as their threshold (the "mode"), which is slightly lower than last year's response. Almost three quarters of respondents (74%) reported limits of 10MB to 50MB. The remainder represented limits as tight as 1MB and as large as half a gigabyte.

15. Does your firm limit the size of outgoing mail? (Last year - 27% Yes, 73% No)

Yes	110	(29%)
No	263	(71%)

Yes	34	(40%)
No	50	(60%)

Yes	53	(28%)
No	134	(72%)

Yes	23	(23%)
No	79	(77%)

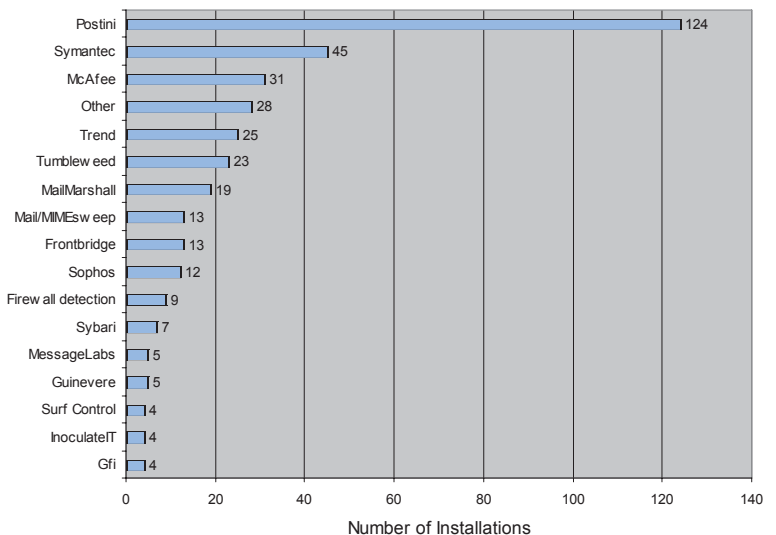
16. If yes, to what size do you limit outgoing mail?

Of the 82 firms reporting an outgoing limit, the most common (24% of respondents) was 20MB (up 10MB from last year.) 50% of respondents cited limits of 15MB to 30MB. The tightest reported limit was 1MB, and the largest allowance (of those who set limits at all) was 250MB.

18. Based on a scale of 5 to 1, with 5 being "very satisfied" and 1 being "unsatisfied, how satisfied are you with this product? (Only those products with 5 or more responses are reported, and the averages are shown below.)

MessageLabs	5.00	Tumbleweed	4.18
Postini	4.71	Trend	4.16
FrontBridge	4.69	McAfee	4.13
Sophos	4.60	Sybari	3.67
Firewall detection	4.33	Mail/MIMEsweep	2.50
MailMarshal	4.26	Guinevere	0.50
Symantec	4.24		

17. Which product does your *initial* scan of inbound e-mail?  
Anti-Virus Initial Scan



**All Firms Combined**

**200 Attys & Over**

**Firms 50 to 199 Attys**

**Firms under 50 Attys**

19. Do you have a *second* virus-scanning system for inbound e-mail? (Last year - 47% yes, 53% No)

Yes	273	(74%)
No	94	(26%)

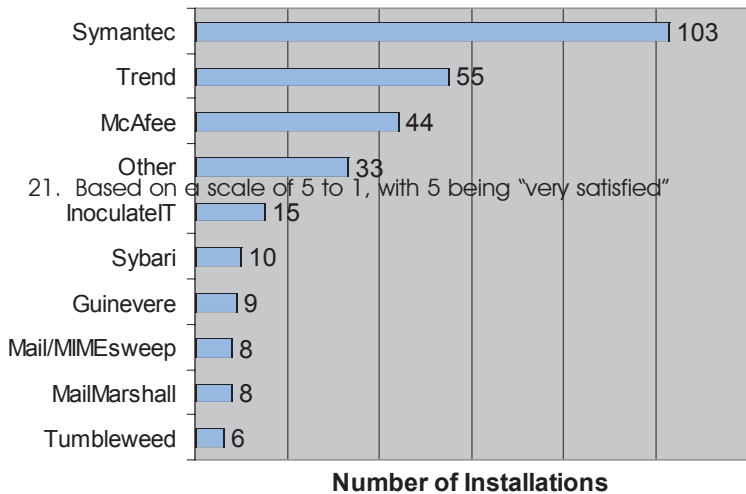
Yes	68	(81%)
No	16	(19%)

Yes	137	(74%)
No	49	(26%)

Yes	68	(70%)
No	29	(30%)

20. If yes, which product does the *second* virus scan of inbound e-mail?

**Anti-Virus Second Scan**



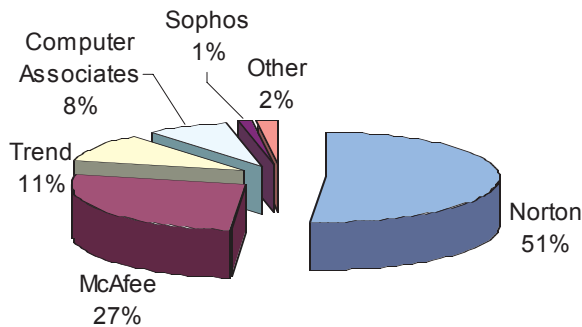
21. Based on a scale of 5 to 1, with 5 being "very satisfied"

and 1 being "unsatisfied, how satisfied are you with this product? (Only those products with 5 or more responses are reported, and the averages are shown below.)

Sybari	4.60	Guinevere	3.56
MailMarshal	4.50	Mail/MIMEsweeper	3.38
Symantec	4.21	Tumbleweed	3.33
Trend Micro	4.05	InoculateIT	3.13
McAfee	3.73		

22. What brand is your primary *desktop* computer anti-virus software? (274 responses)

**Desktop Anti-Virus**



23. Did your firm suffer any computer network downtime in the last 12 months as a result of a computer virus? (Not polled last year)

Yes	70	(19%)
No	305	(81%)

Yes	30	(35%)
No	55	(65%)

Yes	26	(14%)
No	161	(86%)

Yes	14	(14%)
No	89	(86%)

24. Do you filter e-mail based on word content (lexical scanning, e.g., offensive language)? (Last year - 53% Yes, 47% No)

Yes	233	(62%)
No	144	(38%)

Yes	56	(66%)
No	29	(34%)

Yes	122	(65%)
No	67	(35%)

Yes	55	(53%)
No	48	(47%)

All Firms Combined

200 Attys & Over

Firms 50 to 199 Attys

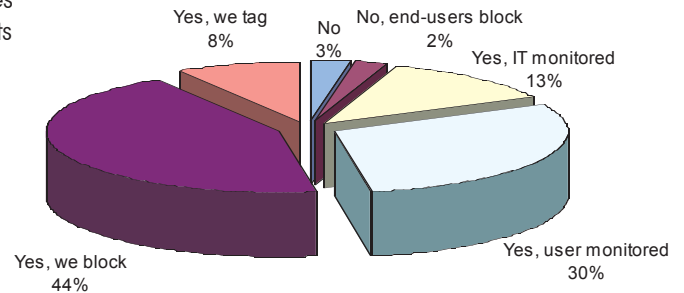
Firms under 50 Attys

25. Do you have an automated spam blocking/filtering system in place?

The choices available in the survey were:

- ~ Yes, and we block spam
- ~ Yes, but we tag the message as spam and send it on to the
- ~ Yes, and users monitor their own quarantine logs for false positives
- ~ Yes, and the quarantine is monitored by IT for false positives
- ~ No, but our end-users maintain their own "block sender" lists
- ~ No

## Spam Blocking



26. If you quarantine, do users monitor their own quarantine queues or is the quarantine queue centrally managed?

(Not polled last year.) (328 Firms responding)

Category	Count	Percentage
Own	197	(60%)
Central	131	(40%)

Category	Count	Percentage
Own	44	(63%)
Central	26	(37%)

Category	Count	Percentage
Own	105	(63%)
Central	63	(38%)

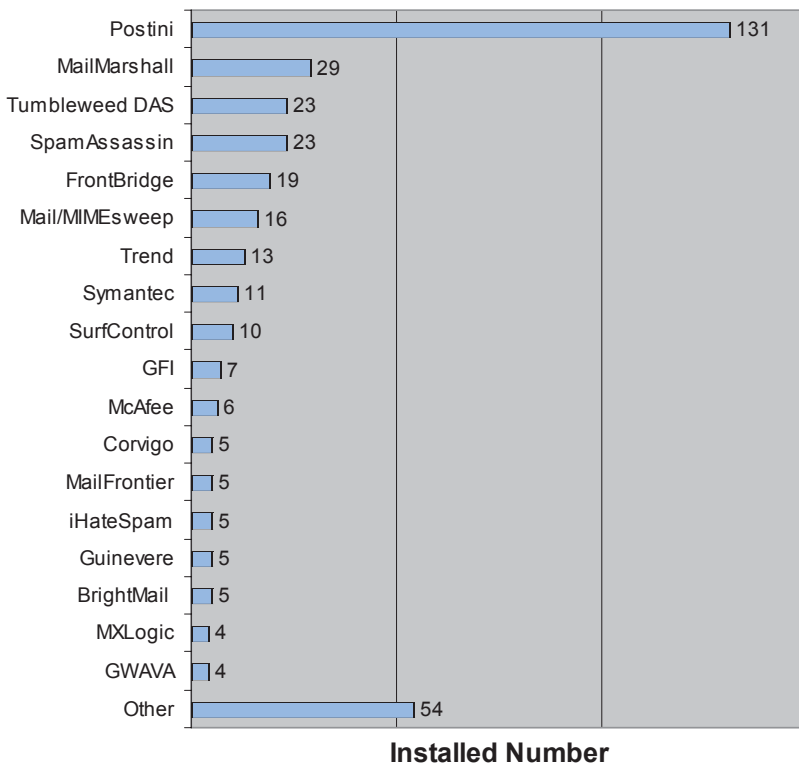
Category	Count	Percentage
Own	48	(53%)
Central	42	(47%)

27. If quarantine queues are centrally monitored, how many hours per week do employees spend reviewing quarantined messages?

Of the 144 firms who reported centrally reviewing quarantined files, half spent three hours or less per week at this task, which is a 25% reduction in time from last year. The overall average was also down about an hour from 5.8 hours per week to 5 hours. 9 firms reported spending 15 hours per week or more and one reported 60 hours. 5 firms responded with "Unknown" or "Very little time" and 1 firm answered, "Too many."

28. If you have an automated spam detection system, what is it?

## Anti-Spam Installations



29. How satisfied are you with this product?

Since many of the products rated by users had a statistically insignificant installed base, the 15 most commonly installed products and their ranking [on a scale of 1 to 5, with 5 being best] are shown below:

BrightMail	5.00
MailFrontier	5.00
Postini	4.74
MailMarshal	4.52
GFI MailSecurity	4.33
Tumbleweed DAS	4.30
FrontBridge (Big Fish)	3.95
SpamAssassin	3.52
McAfee	3.50
SurfControl	3.40
MailSweeper/MIMEsweeper	2.81
Guinevere	2.60
Trend Micro ScanMail	2.08
iHateSpam	1.00
Symantec	1.00

All Firms Combined	200 Attys & Over	Firms 50 to 199 Attys	Firms under 50 Attys
--------------------	------------------	-----------------------	----------------------

30. Do you filter *outgoing* mail for inappropriate content, viruses or spam, etc.? (Last year - 43% Yes, 57% No.)

Yes	158 (42%)	Yes	40 (47%)	Yes	83 (44%)	Yes	35 (34%)
No	218 (58%)	No	45 (53%)	No	106 (56%)	No	67 (66%)

31. Does your firm block or restrict certain types of attachments (e.g., exe, vbs file types)? (Last year - 82% Yes, 18% No.)

Yes	343 (91%)	Yes	79 (93%)	Yes	177 (94%)	Yes	87 (85%)
No	33 (9%)	No	6 (7%)	No	12 (6%)	No	15 (15%)

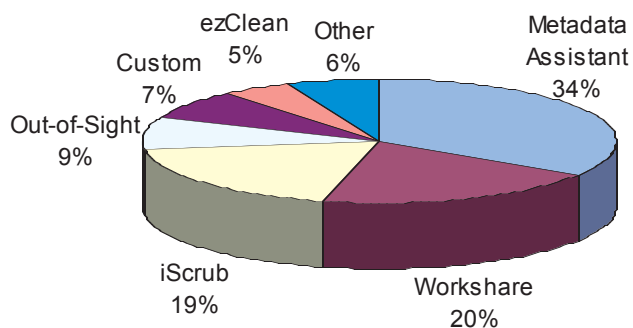
32. Do you use a product to clean metadata on outgoing document attachments? (Not polled last year)

Yes	182 (48%)	Yes	62 (74%)	Yes	89 (47%)	Yes	31 (30%)
No	194 (52%)	No	22 (26%)	No	100 (53%)	No	72 (70%)

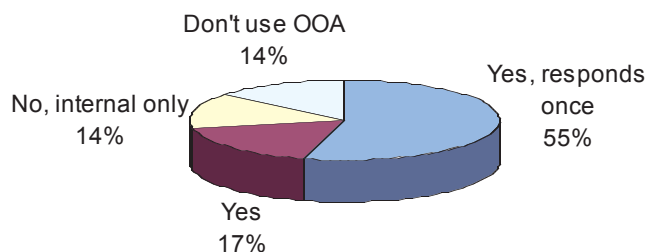
33. If yes, which product(s) do you use? (Not polled last year)

34. Does your firm default the "Out-of-Office" agent to respond to e-mail from outside the firm? (Not polled last year)

### Metadata Cleaners



### Out-of-Office Agent



35. Have you disabled the "automatic completion" feature when addressing (also called "Type Ahead")? (This feature finishes the e-mail address after you type a few letters of the address. It is sometimes disabled to avoid e-mail addressing errors.) (Not polled last year)

Yes	53 (14%)	Yes	12 (14%)	Yes	28 (15%)	Yes	13 (13%)
No	321 (86%)	No	72 (86%)	No	159 (85%)	No	90 (87%)

36. Does your firm have e-mail encryption capability? (Last year - 38% Yes, 62% No)

Yes	131 (35%)	Yes	58 (68%)	Yes	53 (28%)	Yes	20 (19%)
No	245 (65%)	No	27 (32%)	No	135 (72%)	No	83 (81%)

37. If so, which product(s) do you use?

Public key certificates	40%
Tumbleweed	14%
ZixMail	9%
PGP	8%
MailMarshal	7%
Mail/MIME	5%
Lotus Notes	3%
Other	14%

38. Does your firm permit the use of personal instant message (IM) programs like AOL (AIM), Yahoo or MSN? (Last year - 27% Yes; 32% No-Enforced; 42% No, but done anyway.)

Yes	18%
No, enforced	41%
No, but done anyway	41%

All Firms Combined	200 Attys & Over	Firms 50 to 199 Attys	Firms under 50 Attys
--------------------	------------------	-----------------------	----------------------

39. Does your firm use an Enterprise (secure/internal only) instant message program like Microsoft LCS, Lotus SameTime or GroupWise Messenger? (Not polled last year)

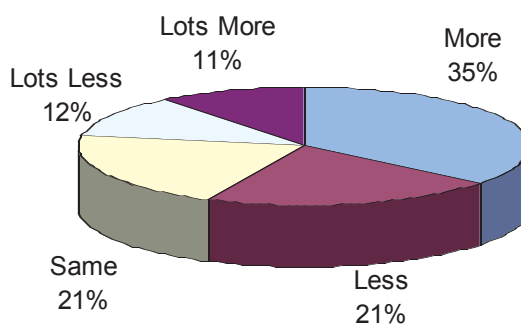
Yes	28 (7%)	Yes	10 (12%)	Yes	12 (6%)	Yes	6 (6%)
No	348 (93%)	No	74 (88%)	No	176 (94%)	No	98 (94%)

40. Does your firm prevent access (via system restrictions) to personal Web-based e-mail services like AOL, Yahoo and MSN? (Not polled last year)

Yes	76 (20%)	Yes	14 (17%)	Yes	46 (24%)	Yes	16 (15%)
No	301 (80%)	No	70 (83%)	No	143 (76%)	No	88 (85%)

41. Compared to 12 months ago, does your firm spend more or less time managing e-mail related issues like spam, viruses, archiving, blocking, etc?

### E-Mail Administration Time



## The Shifting Tactics of Spammers

by Andrew Lochart of Postini, Inc.

Despite the recent enactment of the CAN-SPAM Act by Congress, the epidemic of spam and malicious e-mail carrying viruses and worms continues to spread and grow increasingly sophisticated through techniques that make traditional or first-generation content filtering technology less effective.

### Minimizing Content to Fool Spam Filters

While “hash busting” and Bayesian Poisoning techniques have become familiar to most anti-spam vendors and countermeasures have been incorporated into their products, spammers continue to succeed by becoming even more covert in their tactics. Going beyond fooling the content filter with creative combinations, spammers are taking a more personalized and minimalist approach to get past conventional anti-spam content filters.

The logic behind these spamming techniques is simple: take away or reduce the context of a message to a degree that confuses the content filtering method just enough to allow it to get through. Because filters on servers in an enterprise must handle messages for hundreds or even thousands of users, it is difficult for the IT department to increase the sensitivity of filters to catch these techniques. That’s because increasing filter sensitivity also increases the risk of blocking substantial numbers of legitimate e-mail messages, known as false positives.

More recent spam techniques, for example, use messages that are personalized and unique. These messages display very few typical spam identifiers in its content, making it much more difficult for conventional content-based spam filters to catch and block. Spammers are also putting less content in their messages so that conventional filtering software has less context in which to assess the validity of the message. It is now common to see spam messages with a single word in the subject line and a single URL in the message body, making it virtually impossible for a content-based spam filter to make an accurate decision.



## The Connection Point Battleground

During the first half of 2004, spammers and hackers have also shifted their techniques away from message gimmicks to focus more on the SMTP connection point in their endless quest to overcome content-filtering technology. This change in spamming tactics does not bode well for any organization that must rely on content-filtering technologies to protect its e-mail systems. That's because conventional content filtering cannot block any of these new attacks at the connection point. They must let a message into the system so they can examine its content — at which point the damage from these attacks has already occurred.

## Harvesting Directories and Bringing Down Servers

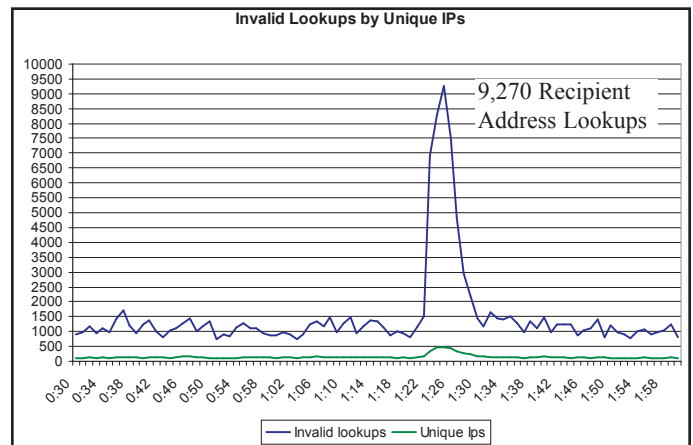
A prime example of this new connection point threat is known as directory harvest attacks (DHAs). DHAs are designed to net spammers lists of valid addresses to which they can send spam or sell to other spammers. It works like this: many mail transfer agents (MTA) typically respond to e-mail delivery attempt requests with a simple “yes” or “no”. If the response is “no,” the sending server gets an error message, since the address is invalid and mail for that address cannot be delivered. If the sending server gets a “yes,” it knows the address is valid and a message can be delivered.

Spammers exploit this functionality to harvest legitimate addresses from a corporate directory by sending a message to thousands or even hundreds of thousands of possible e-mail addresses (e.g., johndoe@yourcompany.com or jdoe@yourcompany.com). Spammers track all of the addresses that do not bounce back or generate errors and consider these valid addresses, which are then compiled into lists that are sold or distributed to other spammers. In fact, it is not uncommon for new users of popular systems like Yahoo or Hotmail to receive spam before they have ever used their new address.

Directory harvest attacks also have a very damaging side effect: consuming enormous amounts of server resources while servers try to cope with DHA probes. Lotus Notes and Exchange servers, for example, generally accept all messages for their domain. This only aggravates the negative impact of a directory harvest attack, because the spammer assumes all

the attempted addresses are valid and thus will send more spam or sell the attempted addresses to others.

Unfortunately, directory harvest attacks are often launched simultaneously from many different computers. The resulting spike in traffic from the directory harvest attack can easily knock a server offline. The diagram below shows a typical case where address lookups will increase by as much as a factor of 10 in just a minute.



## How to Protect Your Firm

Because of the harmful impact from DHAs on system performance, directory harvest attacks must be treated as more than just an inbox or end-user annoyance issue. Directory harvest attacks cannot be stopped by conventional content filtering found in appliances or software since there is no “content.” Nor can spam messages that reduce or eliminate “content” in a message be reliably blocked with content filtering.

The detection of minimal content spam and DHAs must occur in real time, at the SMTP connection point, in order to prevent them from ever reaching the gateway. Fortunately, there are commercially available solutions today that can prevent connection point attacks and block spam from shifting IP addresses. There is also technology that can dynamically recognize the legitimate IP addresses of law firms, for example, and perform a real-time IP address assessment helping to minimize false positives.

It's important that you consider these newly evolving threats as you evaluate your existing anti-spam tools and plan your security strategy for protecting the critical communications so vital to your firm.

# *E-Mail Management: The New Imperative*

*for Law Firms and Legal Departments*

by Neil Araujo of Interwoven

E-mail has evolved into the de facto standard for business communication, and it is through this medium that many substantial business discussions are held and decisions are made. In fact, according to Gartner Group, as much as 75 percent of a company's total knowledge exchange occurs via e-mail. Ironically, although e-mail serves as the default collaborative platform for many companies, it can actually inhibit collaboration. Designed for one-to-one communication, use of e-mail for many-to-many discussions quickly splinters into disconnected and overlapping threads, round-robin decision-making, challenges with version control and other inefficiencies.

To address e-mail overload, law firms and corporate legal departments must first understand the issues involved. Unsolicited e-mail (spam) is a high-profile component of the problem, but other factors can have an even greater cost impact. Matter-related content is being communicated via e-mail; as a result, each user's inbox has become a repository for matter information. This has a tremendous impact on worker productivity because users are forced to search multiple repositories in order to find matter-related information. In addition, an increasing number of large and redundant attachments are pushing e-mail servers to their limits, requiring new IT investment — and risking additional loss of productivity when these servers crash.

Loss of productivity is only the tip of the iceberg. Beneath the surface, countless hours of lost employee productivity are accompanied by loss of business data. If the Outlook Personal folder (PST), stored on an individual's computer is lost (due to hard drive failure, lost computer or employee turnover), many valuable messages may be lost forever.

Although e-mail overload is widely recognized as a problem, there is a tendency for those in charge to accept it as a nuisance and a cost of doing business without recognizing its full implications — and the cost of doing nothing can be severe. The e-mail messages that get lost in overloaded

inboxes aren't just numbers; each represents something: a piece of business knowledge, a part of a process, a potential liability, a risk that needs to be managed, an opportunity that may otherwise be missed.

Most e-mail management solutions today focus largely on logging e-mail messages and archiving them in a dedicated repository that is separate from the e-mail server. Although effective in terms of reducing the load on e-mail servers, this partial solution does nothing to improve worker productivity, which is by far the largest cost element.

## Archiving Is Not E-Mail Management

It is essential to understand the distinction between archiving and e-mail management for productivity and knowledge management. The logging and storage solutions sometimes offered as remedies for e-mail overload may address some retention and deletion problems, but they undermine much of the value of these messages by maintaining e-mail separate from other matter-related content. Stripped of its context, an individual e-mail message is often largely meaningless. Keeping e-mail in the same repository with other matter-related files will preserve the original context that helps users understand and make full use of the knowledge that messages contain.

## Don't Eliminate the Human Factor

Be wary of e-mail management solutions that attempt to automate the filing of e-mail through the use of rules eliminating the need for human involvement. While the notion of sparing users any involvement in the e-mail filing process is attractive at first, there are several reasons why this is not a practical approach. Imagine having to define a set of rules that will file each of the 100,000 or more messages received and sent by a large law firm each day automatically. The effort to develop, test and maintain such a rule base would add considerable cost to any solution.

In addition, as e-mail threads evolve, they may actually morph into entirely new subjects that pertain to a different matter. Since autofiling rules use standard metadata (and sometimes the text within a message) for filing, messages are likely to be auto-filed into the wrong folder, compromising the effectiveness of such a solution.

## Taming the E-Mail Beast

The most effective way to deal with e-mail overload is within the context of a company's overall content management

# CRM to Manage E-Mail

by Barry Solomon of Interface Software

strategy. Storing e-mail in a scalable document management system enables firms to make e-mail part of a unified matter file. This e-mail management process reduces the burden on e-mail servers and transforms e-mail from an isolated knowledge source, visible only to the person to whom it is addressed, into an asset that can be shared securely and easily across offices with both attorneys and clients.

An effective e-mail management process must be capable of automatically capturing and filing inbound and outbound e-mail messages with integrity (making sure that the right messages get filed in the right place) and with minimal intrusion on the user. The key to ensuring effectiveness is to select an e-mail management process that fits seamlessly into users' normal work activities and enables them to file messages from within their e-mail client, desktop applications, Web browsers and wireless devices.

An e-mail management process should enable users to move (via drag and drop) personal folder structures from the Outlook Inbox or PST files into the document management repository, and it should provide smart prompting that can remind users when they forget to file e-mail messages. Look for automatic indexing of both the messages and embedded attachments, allowing users to full-text search documents, e-mail messages and attachments simultaneously — and to profile and display e-mail as e-mail, not documents.

To handle the huge volume of e-mail passing through today's law firms and legal departments, a solution must be scalable enough to handle terabytes of e-mail messages and attachments, and it should provide intelligent duplicate detection to reduce storage requirements.

## Conclusion

Although often taken for granted, e-mail overload is a serious and fast-growing crisis for law firms and corporate legal departments, creating both uncontrollable costs and unacceptable risks. To address it effectively, these organizations must first recognize the role that e-mail plays in their users' work lives and implement an e-mail management solution that makes it simple for users to access both the messages themselves and the related matter content that makes them meaningful.

E-mail is the preferred IT environment for most professionals. And as the volume of legitimate and unsolicited e-mail climbs, lawyers increasingly must spend nonbillable time sifting through their inboxes prioritizing messages, sharing e-mail communications with client team members and storing communications to generate an electronic trail documenting the status of client matters.

## CRM to the Rescue

Taking a proactive approach to this growing problem, savvy law firms are increasingly investing in CRM systems that offer tight integration with their e-mail environments. Benefits of CRM include:

***Identifying unknown e-mail senders** — When an e-mail arrives, to know whether it warrants a quick response or any response at all the lawyer must first determine who it's from and whether the sender is a client or prospect. A button from the CRM system integrated into the e-mail application can instantly identify the sender and retrieve a complete background profile that gives the user all he/she needs to decide whether, how and when to respond.*

***Building a Client History** — Rather than printing messages or saving them in private folders, selected e-mail communications can be automatically saved to the central repository, creating an ongoing client history, with no effort on the lawyer's part.*

***Improving Client Management** — When client team members fail to keep each other informed about the flurry of e-mail communications going back and forth with the client, embarrassing errors or mishaps can occur. By linking e-mail with the CRM system, users can be automatically alerted when important communications occur with clients they are watching, ensuring they always have the latest information.*

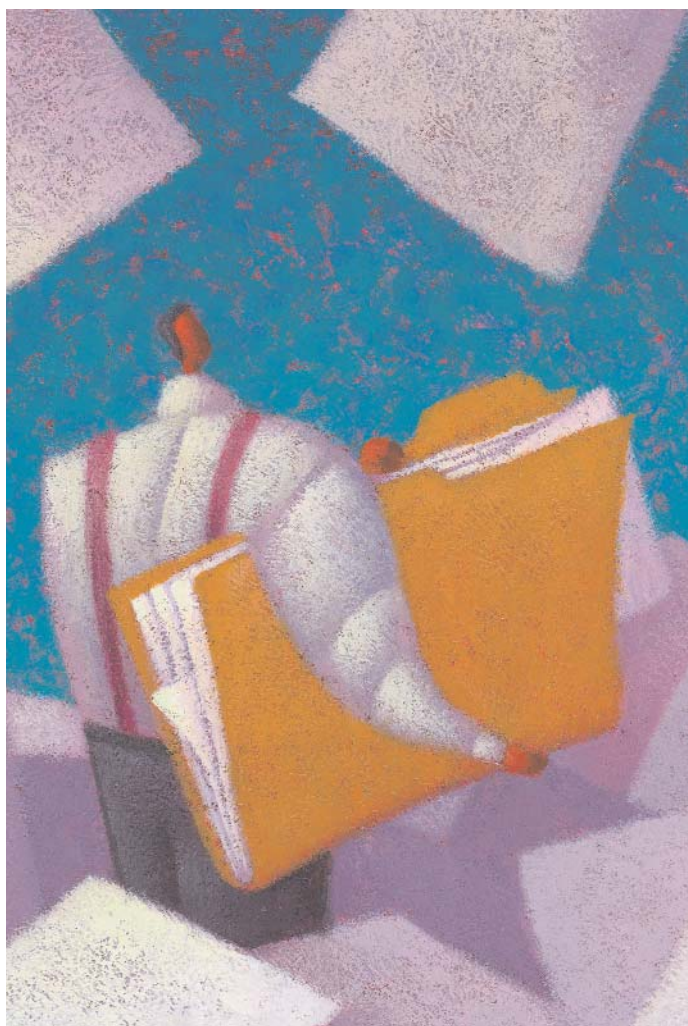
## Conclusion

By investing in CRM platforms that offer sophisticated integration with leading e-mail platforms, firms are discovering the value that relationship intelligence can play in streamlining e-mail traffic and enhancing communication among client team members.

# Website Content Management System

*Doubles as E-Mail Content Generator*

by Sonny Cohen of Duo Consulting



If content is worth posting on a law firm's website, it can and should be promoted to interested constituents. To accomplish this, Vedder Price, with offices in Chicago, New York City and New Jersey, integrated its content management system with its permission-based e-mail system. The result: with a few clicks, news, events or recent articles populating the firm's site can be plucked from the website content management system and formatted into professional-looking e-mail messages.

As at many law firms, the marketing staff at Vedder Price labors to extract newsworthy information from attorneys, stay on top of the changing business environment and communicate information meaningfully. So it made sense for the firm to adopt a system that ensures that this information reaches a broad, yet targeted, audience and that it can be distributed as efficiently as possible.

## An Opportunity to Build in New Features

A revamp of the website provided an opportunity to underlay the new look and feel with a marketing-based content management system (CMS) that could provide new dimensions of flexibility and functionality. Newsworthy and time-sensitive information, as well as periodic publications, could then be easily published to the site.

As part of the website development, the firm embraced an ASP-based e-mail system to conduct permission-based e-mail communication. The system was selected, in part, because its services-oriented architecture permitted a seamless link to be built from the content management system into the e-mail system.

## How the System Works

A link from within the CMS administrative dashboard takes one to an application where the administrator can select content for inclusion based on three criteria. Here are the important steps:

**CHRONOLOGY.** *Content can be selected by either a date range or simply from the last time content was pulled from any category.*

**EXPERTISE.** *A second option identifies the content focus. For many law firms, these are defined as Practice areas such as Corporate Transactions, Bankruptcy, etc.*

**SPECIAL MIX.** *The third option is to send interested contacts information relating to a specific area of law but with a variety of content from among the categories of seminars, news and publications (all or any).*

Upon selection, a query returns a list of content by title within the CMS that satisfies the criteria. Marketing department personnel can further fine-tune the selected content by deselecting items they wish to exclude. In final preparation for moving the content into the e-mail system, the last screen permits the display order of the information to be altered.

Within the e-mail application, a template is selected that's consistent with the chosen content. The firm's Construction Law Practice, for instance, has its own branded e-mail template, populated with the selected content from the CMS application via Web services. The template additionally includes sections in which personalized salutations and static content (*e.g.*, general announcements and signatures) may be added to complete the e-mail communication.

The format of the dynamic content in the message comprises a subject heading (*e.g.*, publications) followed by the list of hyperlinked titles that refer to the page on the website where the full content resides. There is also a brief text abstract prepared from the first lines of the body text.

These few simple steps conclude with the preparation of a subject line, the selection of the targeted list from the opt-in permission-based list and the sending of the e-mail message.

### Monitoring and Tracking

To allow for the real-time assessment of results, backend metrics track the performance of the e-mail message. Deliverability, e-mail opens and click-through rates are all of paramount concern. Marketers can note the topics in the message that stimulated the most interest, as indicated by the rate at which those topics were viewed. Additional informative tracking takes place within the website's server logs and can be mined with minimal effort. It's easy, for example, to monitor an e-mail subscriber's arrival at a linked page on the website and track movement from this page to other content pages within the site.

Vedder Price's system automates a number of individually simple, if arduous, processes. Anyone in the firm can manually repurpose Web content into an e-mail communication; however, with the integration of the content management system with the e-mail marketing system, the entire process can be completed in minutes by individuals with simple word processing skills. Relevant and up-to-the-minute content is identified, and an e-mail template is populated. Targeted permission-based lists are selected, and the e-mail message is delivered. Backend metrics monitor the performance of the entire process.

### Unqualified Success

Since the program's inception, the firm has conducted over 30 e-mail campaigns and reached over 8,000 individuals. Unsubscribers have been few, and the number of recipients who open the e-mail messages is over 50 percent. Further refinements planned include a tighter integration between the e-mail system and the content management system. But without question, the system is currently working well and beginning to pay marketing dividends.

### Development Tools for CMS/E-Mail Integration

The Marketing/Content Management System is built using Macromedia's Cold Fusion MX Application Server on a Microsoft SQL Server 2000 database, adhering to Fusebox methodology.

The ASP e-mail system is provided by ExactTarget. Called ExactTarget Foundation, the next-generation e-mail marketing software platform is built on the Microsoft .NET architecture. The .NET architecture delivers new features and functionality, improved performance, security/reliability and accelerated product development cycles.

## About the Authors

---

**Neil Araujo** is Vice President of WorkSite Product Management at Interwoven (formerly iManage). One of the original founders of Netright Technologies, the developers of the iManage document management software, Neil has been involved in developing products for the legal industry for the past nine years. He can be reached at [neil.araujo@interwoven.com](mailto:neil.araujo@interwoven.com).

**Sonny Cohen** is Law Firm Marketing Strategist for Duo Consulting. Duo Consulting offers strategy, design, development and marketing services to businesses and organizations serious about creating great Internet applications. Duo focuses on law firms, business-to-business and services business, non-profits and the public sector. Sonny can be reached via e-mail at [scohen@duoconsulting.com](mailto:scohen@duoconsulting.com).

**Todd Corham** is the Director of Information Services and Technology at Lowenstein Sandler PC, a 200-attorney firm in Roseland, New Jersey. He has been involved in legal technology for over 20 years. Todd has conducted and compiled LawNet's e-mail survey for the last three years and was a panelist on LawNet's Web conference on E-Mail Retention and Policies. He has worked as a training consultant specializing in legal technology and has written and presented for various industry groups and publications. He can be reached at [tcorham@lowenstein.com](mailto:tcorham@lowenstein.com).

**Andrew Lochart** is responsible for Postini, Inc.'s worldwide product marketing activities, including corporate positioning/messaging. He has amassed extensive messaging industry experience, having worked in a variety of senior marketing management roles at HP OpenMail, Mirapoint and Sendmail during the past decade. Andrew can be reached at [lochart@postini.com](mailto:lochart@postini.com) or 650.482.3161.

**Barry Solomon** is a lawyer and Executive Vice President of Interface Software Inc., the leading provider of CRM solutions for law firms. A recognized leader in areas of technology in the professional services sector, he focuses on corporate strategy, product development and emerging markets. Barry is a frequent speaker at industry conferences and a prolific writer for business, technology and trade publications. He can be reached at [bsolomon@interfacesoftware.com](mailto:bsolomon@interfacesoftware.com).

---

LawNet, Inc.  
2110 Slaughter Lane, #115  
PMB 149  
Austin, Texas 78748



PRST FIRST CLASS  
MAIL  
U.S. POSTAGE PAID  
PERMIT NO. 1149  
AUSTIN, TEXAS

• Address Service Requested