PERMESSA™
::Take Control of Enterprise Messaging

6 BEST PRACTICES THAT REDUCE EMAIL OVERLOAD AND COSTS

By Stefan Mehlhorn, President and CEO, Maria Tricca, Marketing Manager, and Roger Matus, Vice President of Marketing, Permessa Corporation

A few proven email management best practices can reduce email impact by up to 80% — without affecting employees or the bottom line.

There are six practical best practices that most enterprises can implement to reduce the impact of email by up to 80%, without changing the culture or operations of the business. These steps will significantly reduce storage and bandwidth costs, and help reduce the information overload that is stifling employee productivity.

Email currently consumes vast amounts of IT resources.

- The average corporate email user sends and receives 149 valid emails per day, according to Osterman Research, a well regarded messaging research firm. At a 10,000 person organization, these messages currently consume 51.2 gigabytes (GB) of storage per day, Osterman says. By 2010, they predict that the storage need will grow by 60% to 81.9GB per day. Not surprisingly, message volume is a major IT concern. 59% of organizations indicated that messaging storage growth is a serious or very serious problem, according to a survey conducted by Osterman.

- 30% of a knowledge worker's day is consumed by too many messages and too many interruptions, according to Basex, a frequently quoted New York-based research firm. They named this information overload as the "Problem-of-the-Year" for 2008.

As the number and size of messages grow, they will choke existing email systems, drive up the cost of mandatory email archiving and burden knowledge workers, unless the messages are controlled. Unfortunately, most companies deal with email issues the same way. They invest in more servers and bandwidth, issue written policies about appropriate email usage, implement simple restrictions — such as on attachment sizes — and keep their fingers crossed that there won't be a system outage.

However, there are ways to manage email more efficiently without impacting users or business operations. According to research by Permessa, based on 15 years of experience with leading global enterprises, 80% of email impact comes from just 4% of messages which, in turn, typically come from just 1% of the user community.

Here are some examples of manageable events that consumed significant resources. In each case, it is a very small number of employees that had a very big impact:

- At a leading financial services firm, one user regularly sent a 2MB newsletter to every employee. The user included a copy of the corporate logo on the top of the email. Unfortunately, it was a high resolution image. Simply replacing the logo with a smaller version saved 1.5 terabytes (TB) of storage every year.

- The email servers at Total Oil Trading SA (TOTSA) stalled for minutes at a time and impacted service level commitments. It turned out that a few traders periodically sent broadcast emails with large attachments. With minimal effort, TOTSA created an application that significantly shrunk these emails by storing the attachments in a database, restoring email performance to all.

- Linde Gas, a European-based company with more than 16,000 employees, found its email volume increasing too quickly. The company determined that many workers sent 600-700MB of email to themselves each week for storage. Once the users were provided with alternative, lower cost email storage options, the company saved tens of thousands of dollars each year.

In each case described above, the solution to the problem was simple and did not affect the users or the operation of the business.

Here are Best Practices you can follow to keep your messaging system humming — without causing major upheaval to your infrastructure, employees or bottom line:

Best Practice 1: Control Reply-to-All

When used correctly, the "Reply-to-All" button enables a user to provide relevant comments back to the original email author and other recipients listed in the TO: field. When used incorrectly, the Reply-to-All button can lead to an email storm that consumes storage and bandwidth.

In one widely reported incident in October 2007, a subscriber to the U.S. Department of Homeland Security's "Open Source Intelligence Report" wanted to update his email address. Instead of sending his email to the administrator by hitting Reply, he

accidentally hit Reply-to-All. His message was sent to the entire DHS distribution list. In the hours that followed, many subscribers responded, also using Reply-to-All.

By the end of the day 7,500 DHS employees generated more than 2.2-million email responses that slowed email processing and filled mailboxes. In addition, once-private email addresses, phone numbers and titles of military personnel and government workers were revealed to the entire list.

While most Reply-to-All gaffes are more contained, they can have far-reaching consequences that include:

- An overloaded messaging system that impacts Service Level Agreement (SLA) commitments.
- Lost employee productivity as individuals spend time reading, responding to or deleting the Reply-to-All banter.
- A huge amount of wasted storage space on the email server and the legal compliance archiving system.

Best Practice: Put in place an enforceable email policy that controls the number of recipients in an email message. Certain people such as corporate officers and security personnel may deserve unlimited access. It may make sense to provide a simple prompt to confirm before sending an enterprise-wide email. Selected email accounts, such as list servers and those used to send corporate newsletters may also have no limits.

But, other employees can be managed. Department heads may have limits that are near to the size of the largest departments. Individual employees may have limits from 20 to 50 recipients, depending upon the organization.

This simple practice, which requires control by sender, can reduce the Reply-to-All problem to a reasonable number of messages that will not impact service or corporate operations.

Other future technologies will augment screening by message size for even more effective filtering. For example, natural language content inspection will be able to detect whether an authorized sender accidentally sent a suspect message. Confirmation may be requested in real-time. These capabilities are still too error-prone to be practical for deployment. But, extensive work in these areas is underway.

Best Practice 2: "Smart" Size Limits

In an attempt to curb overall email volume, it is common for organizations to limit the size of messages as they are sent. Often the limit is 5-10MB for external and 10-20MB for internal mail.

Setting "as sent" size limits seems like a good idea. But, they never achieve the desired results for two reasons:

First, "as sent" size limits aren't based on the total burden an email places on the network. Permessa's extensive analysis of messages sent at large enterprises shows that a significant burden comes when a medium sized message is sent to a list of recipients.

The chart below illustrates the typical real message size distribution at an enterprise and the resulting volume impact on the network.

As expected, the highest number messages are ordinary messages, as shown by the largest blue bar. But, the total impact on the network is small, as shown on the gold bar.

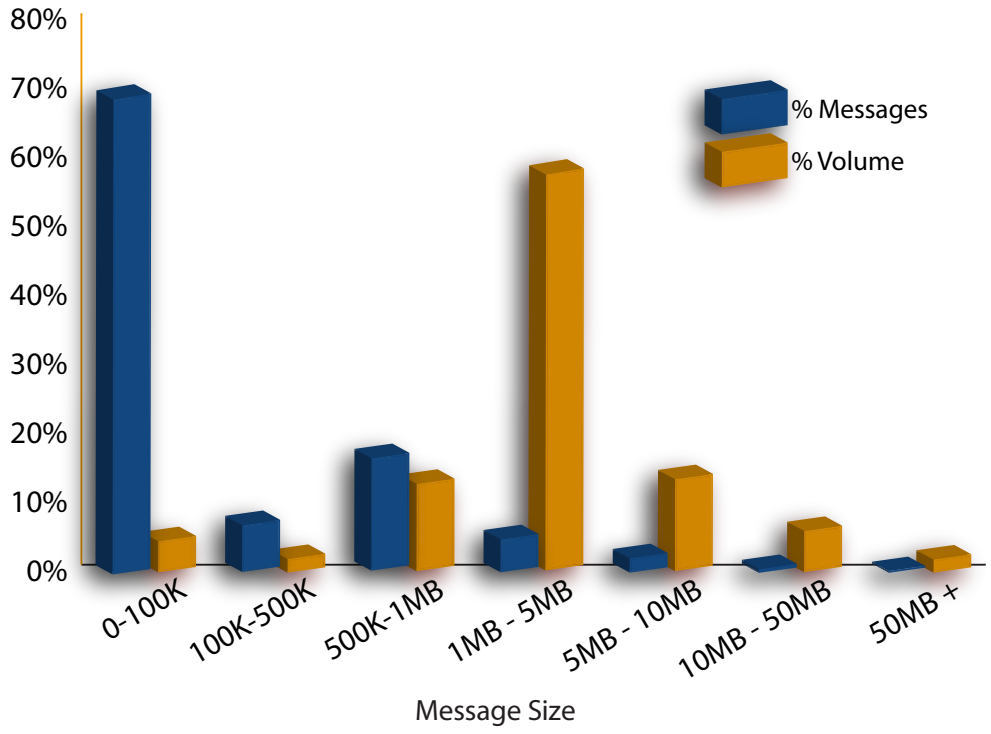
The surprise to most organizations is the impact of messages between 1-5MB. These are often sent repeatedly to many recipients. As a result, these messages are the real burden on the infrastructure. (75% of the total data volume is caused by messages <5MB.)

On the other hand, extremely large messages have a relatively small impact because they're usually sent to small numbers of recipients and there are fewer of these messages overall.

The other reason for avoiding "as sent" size limits is that they can impact business operations. It is no longer uncommon for a sales person to need to send a 12MB Microsoft PowerPoint presentation to a customer. If it is blocked and delays a customer purchase, the well-intended IT rules could hurt revenue.

Best Practice: Create "smart" message size limits based on the total impact of a message rather than the size "as sent."

Infrastructure Impact by Message Size



Best Practice 3: Stop Attachment Ping-Pong

Two years ago, a typical email message might use 20KB of storage. Now, 1MB Microsoft Office attachments are commonplace — a 50-fold increase. Analysts predict attachment types such as video will make 50MB to 200MB messages common in the next few years. This is another 50-fold increase in attachment size.

An attachment, which may not be large enough to trigger smart message size limits in a single email, can become significant if colleagues include the attachment when replying. Each time the attachment is included, it racks up undue network and storage consumption. For example, a single 12MB PowerPoint presentation that has been sent back and forth three times between four people can cause as much as 108MB of unnecessary traffic.

Best Practice: Modify the default mail template so that users are provided with the option to reply to a message without including the original attachment. Expect that future systems will automatically delete previously received attachments when a Reply or Reply-to-All button is used.

Best Practice 4: Prevent Mailing Group Misuse

Mailing groups, sometimes called distribution lists, are essential for communicating with large numbers of users and team collaboration. But when lists are misused, either intentionally or unintentionally, the impact can be significant.

Misuse can occur when unauthorized workers use mailing groups to send inappropriate messages to large numbers of people. For example, in the wrong hands, distribution lists can turn into a conduit for airing personal grievances.

Mailing groups used by the wrong person can also contribute significantly to colleague spam. There are many stories of people sending messages about "food in the conference room," "selling Girl Scout cookies," and other trivial matters to an entire company. While well-intended and appropriate for teams, these messages can waste time, clog mailboxes and consume archiving resources.

Distribution lists also present an IT management challenge. Typically, corporate managers and executives make a request to IT in order to set up a new group. However, expiration dates are rarely set. As a result, groups accumulate over time, which makes it next to impossible for IT to manage or keep them current.

Best Practice: Limit the use of mailing groups to authorized lists of personnel. Each group can be limited by job level, department, job function, or named senders. Others should not have the opportunity to easily send a mass mailing.

Set expiration dates when groups are created or periodically identify inactive mailing groups that can be eliminated. Once these groups are identified, be sure to notify users before they are retired. This simple step, which can reduce the number of complaints from affected parties, is often overlooked by IT.

Email management systems can accumulate statistics that aid in retiring unused mailing groups. An effective solution can help to reduce corporate liability risk and storage requirements, as well as increase employee productivity.

Best Practice 5: Purge Expired Mail Accounts

Employees may come and go, but sometimes, their email accounts remain active for years and continue to consume gigabytes of storage space. Most IT organizations archive mailboxes when an employee departs. But the accounts are not deleted so that managers can see new incoming mail messages.

For a 10,000-person organization with an average employee yearly turnover rate of 23.4%, these storage requirements can add up quickly. Using Osterman Research's figure that employee mailboxes for 10,000 users will consume 81.9 GB per day by 2010, a full year of data could reach 21TB. If 2,340 employees (23.4%) leave the organization each year, the impact of their stale mailboxes could be nearly 4.9TB for each year of data. Of course, many mailboxes contain many years of mail. So the storage number may underestimate the impact of stale mailboxes.

Best Practice: Eliminate stale mailboxes. One way to do this is to identify employee email accounts with no sent mail. If an employee mailbox has incoming but not outgoing mail for an extended period of time, there is a good chance that the employee is no longer using the mailbox. It is important to use common sense in selecting the mailboxes to eliminate. For example, some marketing mailboxes are intended only to receive email. An email management system can automatically generate reports that identify email accounts with no sent mail. These systems can also show exactly how much storage space email accounts are consuming and provide ongoing statistics about mail volumes to help use valuable storage space efficiently.

Before deleting a user account, it is important to check with the employee's manager and the Human Resources department. The manager may still need to monitor incoming mail, rather than having it automatically rejected. Human resources and Legal can also verify that an employee has left the company and that there are no legal obligations to maintain the files.

Best Practice 6: Educate High Impact Users

Many consultants recommend training all employees on email policies. Employees, however, often ridicule the training and management is concerned about the most effective use of employee time.

Email training can have high impact when focused on the users who create the largest problems instead of subjecting the entire organization to lengthy training sessions.

As discussed earlier, 1% of employees are responsible for 4% of messages that cause 80% of the email impact. That means that training time is best spent on the 1%. It can also be focused on the topics that are most critical.

Real-time policy enforcement alerts sent

to users who attempt to send a message that violates email policies can provide ongoing education and improve compliance.

Best Practice: Provide basic email policy training to all employees, but reserve detailed training for the 1% of employees who create the most problems. Showing examples of what is happening within the organization will increase the effectiveness of the training.

Email policy enforcement solutions can reinforce the training by automatically notifying employees when email policies are violated.

CONCLUSION

These six best practices can help organizations solve 80% of the typical email management problems. Commercially available email management tools, such as those offered by Permessa, can help organizations to implement these best practices that deliver significant benefits without negatively impacting the enterprise:

- **Best Practice 1:** Control Reply-to-All abuse by limiting the number of recipients in an email message. Limits may be set by user or group.
- **Best Practice 2:** Focus on the overall impact of messages rather than taking a one-size-fits-all approach to "as sent" message size limits. Individual messages with large attachments do not have the biggest impact. It's the medium-size messages sent to large distribution lists that pose the real problem.
- **Best Practice 3:** Stop attachment ping-pong. Configure mail templates so they don't automatically add original attachments when users reply to messages.
- **Best Practice 4:** Prevent mailing group (distribution list) misuse. Limit the use of mailing groups to authorized personnel.
- **Best Practice 5:** Eliminate stale email accounts with no sent mail. These accounts typically signal that an employee is no longer with the company, allowing you to recover valuable messaging storage space.
- **Best Practice 6:** Educate the highest impact users about their email usage. Addressing the 1% of users with the highest impact can have a significant and positive impact.

Rev. D