

Recession Proof Your Business Email Through Outsourcing

An Osterman Research White Paper

Published December 18, 2008

SPONSORED BY

USANET[®]
A Perimeter eSecurity[™] Company



Executive Summary

Email is critical on a number of levels and is becoming more so over time:

- Email is the most important communications tool in most organizations, more important than the telephone, instant messaging, fax, video, etc.
- Email is the single most important repository of critical business information, containing contracts, proposals, purchase orders, client communications, statements of corporate policy, etc.
- Email is the primary file transport tool for most users, used to send a wide and growing variety of documents. While many organizations have FTP or other file-transport systems in place, email's ubiquity and ease of use have made it the de facto file transport system for the vast majority of users.

Email's importance is overshadowed only by the formidable task of keeping everything up and running as close to 24x7 as possible, adding new capabilities to the email infrastructure over time, protecting against new and ever more virulent threats, and ensuring that email can support current and future business processes. These tasks are made all the more difficult by the fact that the cost of managing email will become more expensive over time.

Given the difficult economic times that began in Summer 2008 and that will extend through at least 2009, organizations of all sizes and in all industries are faced with the difficult task of maintaining robust email capabilities and adding more capabilities over time, while reducing costs in a way that we have not seen since email became the critical business tool it is today.

Email's importance is overshadowed only by the formidable task of keeping everything up and running as close to 24x7 as possible.

An alternative that many organizations should consider is the use of a hosted email service. Using such a service can reduce the costs of managing email, make these costs more predictable, offer a higher level of service, speed the addition of new capabilities as demand arises, and free IT staff for tasks that will provide more value to the organization.

This white paper sponsored by USA.NET, offers a variety of points for decision makers to consider as they evaluate how to improve email in an era of tightening budgets.

Managing Email in Difficult Economic Times

EMAIL USE IS GROWING

Despite the continued and growing use of non-email technologies in the workplace – instant messaging, voice etc. – email use continues to grow. Osterman Research has found that email use is growing at 20% per year or more in some organizations. Further, because of increasing use of attachments, larger attachments that include multimedia content, increasing use of email as a repository for critical business records, and greater dependence on email as the de facto file transport mechanism in most organizations, message stores are growing in excess of 30% per year – in some organizations, growth is increasing at more than 50% per year.

Users are increasingly reliant on email, as well. A recent Osterman Research survey found that users in smaller organizations (up to 1,000 users) spend one-third of their day doing work in their email client; in larger organizations, that figure is 40%. The same survey also found that 44% of the information that users in smaller organizations need to do their work is somewhere in email; for users in larger organizations, that figure is 48%.

The result is that email systems are becoming more difficult to manage from a purely functional perspective – they send and house more information, more of this information is of a business-critical nature, and users are increasingly reliant on email as the primary business tool that they use on a daily basis. This makes service interruptions and an inability to support user demands less and less tolerable.

THREATS ARE BECOMING MORE DIFFICULT TO ADDRESS

At the same time, the email landscape is becoming an increasingly threatening place in which to work. Consider:

- Spam volumes are increasing over time, in some cases very rapidly around certain times of the year like Halloween or Christmas, or because of specific events, such as the US presidential election.
- Spammers are becoming more sophisticated, sending blended threats that include a link to a Web site that will automatically download malware, such as keystroke loggers.
- Social engineering techniques are becoming much more common, and include threats like Facebook “friend” invitations and requests.
- Malware is becoming more difficult to detect and remediate. Gone are the days when “splashy” threats like Melissa or the I Love You virus infected corporate systems. Instead, today’s threats are stealthy, designed to intercept sensitive and confidential information and operate well below the radar.
- Spyware/adware is increasingly common, designed to track user behavior or otherwise infect users systems with monitoring or tracking tools.

- Phishing, spearfishing and whaling are becoming more common. These threats, designed to fool users into providing bank account information, login credentials or other sensitive information, are becoming more sophisticated over time and are able to trick a large proportion of users into handing over sensitive information.

THE GROWING VOLUME OF INBOUND SPAM AND MALWARE OFTEN OVERWHELMS ON-PREMISE SYSTEMS

While a standalone, on-premise email security infrastructure can provide a good defense against a variety of threats, sudden increases in spam can overwhelm an on-premise infrastructure. For example, one major spam processor reported an increase in spam volume of 78% during one 24-hour period in November 2008.

When spam and malware volumes increase suddenly, there can be quite serious consequences:

- The messaging infrastructure bogs down under the weight of the newly increased messaging load, resulting in slower email delivery and, in some cases, outright crashing of mail servers.
- IT administrators scramble to address the problem by adding security appliances or servers to solve the myriad problems that arise from the sudden increase in message volume. Help desk costs also increase as users wonder why their mail is not getting through, why they are not receiving email they are expecting, and so forth.

The key is adding critical security defenses on a limited or stagnant budget – a challenge most companies will face during 2009.

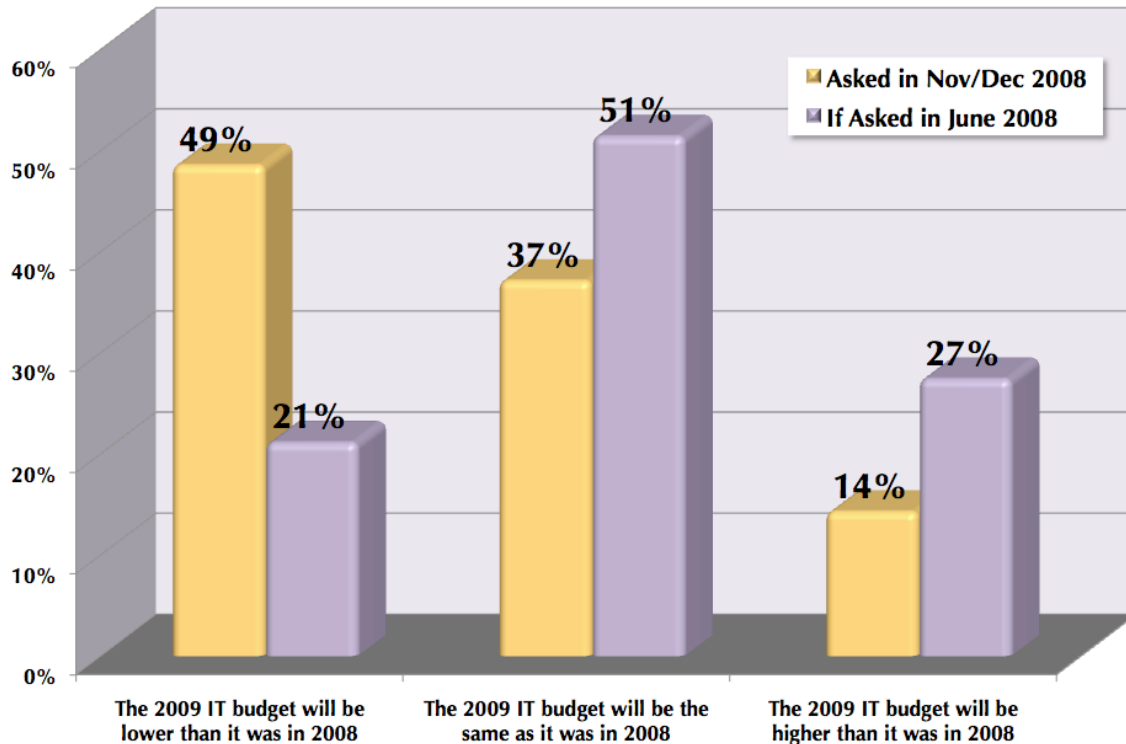
IT departments can address this issue by simply adding lots of excess capacity in anticipation of a spike in spam and malware. However, the cost of adding this spare capacity for random spikes is expensive and difficult to justify, particularly in difficult economic times. Plus, even the best-laid plans might not anticipate the heaviest spam spikes. The key is adding critical security defenses on a limited or stagnant budget – a challenge most companies will face during 2009.

IT BUDGETS WILL BE TIGHTER IN 2009

Two Osterman Research surveys conducted in November and December 2008 found that IT budgets will clearly be getting tighter in 2009 as a result of the current economic problems being experienced by companies worldwide. For example, as shown in the following figure, almost one-half of organizations will have a lower IT budget in 2009 than they did in 2008 – only one in seven organizations will have larger IT budgets. We also asked respondents to these surveys – decision makers in small, mid-sized and large organizations – how they would have estimated their 2009 IT budget in June 2008, well before the economic crisis reached its worst. The figure shows that the current economic

problems have significantly increased the number of organizations that have lowered their IT budgets.

2009 IT Budgets Compared to 2008



Note: totals do not equal 100% due to rounding error

THERE WILL BE MORE FOR YOUR IT STAFF TO DO IN 2009

Certainly, spam and malware will be getting worse and need to be addressed continually by your IT staff.

Even though the economy is slowing, requirements for new defenses are not – to stay competitive and keep your workforce productive, your defense against new threats cannot stand still. However, there will be significantly more for your IT staff to do in the months and years ahead than just manage email security. Among these tasks are:

- **Archiving for compliance**

Archiving for compliance purposes is becoming a legal and statutory necessity. Organizations must deploy archiving systems to preserve not only their email content, but all sorts of other content, including Microsoft Office files, databases, output from CRM and ERP systems, instant messaging conversations, content from collaboration systems, wiki and blog postings and any other content that might be needed during a legal discovery effort or in some way connected with litigation support or regulatory compliance.

- **Collaboration and unified communication**
Organizations will need to deploy collaboration and unified communication systems. Osterman Research surveys indicate that organizations are increasingly deploying collaboration tools and unified communication systems to support user demand to do more with less. These tools offer the promise of greater employee efficiency and productivity while reducing costs. Senior managers in a growing number of companies are convinced of the benefits associated with improved collaboration and unified communications and will continue to drive demand for these capabilities.
- **Real-time communications**
Microsoft Office Communications Server, Lotus Sametime and a growing variety of other real-time communication tools – in addition to the large number of consumer instant messaging systems already in place – are becoming more commonly used. IT departments will increasingly be called upon to deploy enterprise instant messaging capabilities, either as standalone tools or, more commonly, as part of unified communication systems.
- **Corporate governance management**
Corporate governance is becoming a much more top-of-mind issue for corporate decision makers. While financial services companies will clearly be in the crosshairs of many government regulators in the months and years ahead, most organizations will face increased scrutiny and must implement systems that will help them comply with increased oversight.
- **Mobile messaging**
The use of mobile devices, as well as a growing trend toward employee mobility in general, are driving demand for mobile infrastructure that can support these users. IT departments will be required to deploy and manage these capabilities to support the growing number of mobile users in their organizations, many of whom have strong preferences for specific devices.
- **Business continuity and disaster recovery/avoidance**
Email and other communication systems are becoming increasingly critical to the way that people work. As a result, these systems must stay up and running virtually 100% of the time, requiring IT to implement disaster recovery and business continuity capabilities that will ensure the availability of critical business systems.

Why Consider Using a Specialist Provider?

MARKET OVERVIEW

Osterman Research forecasts that the market for hosted email will increase significantly over the next several years, from 10% of all corporate mailboxes among mid-sized and large organizations in North America in 2008 to 22% by 2011. Penetration of hosted email among smaller organizations will be even greater for reasons discussed below.

COSTS CAN BE LOWER

One of the primary reasons that many organizations will adopt hosted email is that often the cost of doing so is lower than the total cost of managing an infrastructure in-house. Osterman Research has found that for smaller organizations, as well as for many larger ones, the cost of managing an in-house email infrastructure is higher than if a specialist, third-party provider manages the service. This is largely due to the fact that the costs borne by a hosted provider for IT staff, servers, facilities, redundancy, etc. are spread out over a much larger base of users, resulting in relatively low costs per seat.

COSTS ARE MORE PREDICTABLE

Use of a hosted email provider results in more predictable costs for several reasons:

- Growth in messaging storage is the leading on-premise email management problem, requiring organizations to periodically deploy more storage as demands increase. Use of a hosted provider, on the other hand, does not necessitate increases in storage, particularly when a provider is used that offers substantial amounts of storage for a fixed fee per month.
- Costs for hosted services are often lower than for on-premise services. The predictability of hosted services costs reduces budget risk.
- Some upgrades require significant and sometimes unpredictable maintenance and support costs, such as the requirement to use 64-bit hardware for an Exchange 2007 upgrade. This type of upgrade requires not only new hardware, but a resource-intensive “forklift” upgrade process.
 - As noted above, spam and malware spikes can force organizations to scramble as they add new capacity, resulting in procurement, deployment and additional management costs for the newly added infrastructure. A hosted provider, on the other hand, simply absorbs these costs. They might have to add capacity during particularly heavy increases in spam or malware, but their customers will continue to pay the same fee.
 - Operating a heavily layered defense is expensive when doing so on-premise. Here again, the economies of scale enjoyed by hosted providers, coupled with their distribution of infrastructure costs over a large number of users, gives hosted providers a distinct cost advantage compared to most on-premise deployments.
 - Hosted providers manage all of their capabilities for a constant price during a contract period. This allow their customers to accurately predict the cost of email management over at least the term of the contract period – several years in some cases.
 - The costs are also known for enhanced services not currently used, so that as business requirements change, organizations can budget at known costs before a particular service is “turned on”. Because the price of specific services are known before they are

activated, there are no unknowns about the cost of adding capabilities, reducing the risk of adding new services.

SERVICE LEVELS ARE TYPICALLY HIGHER THAN FOR ON-PREMISE SYSTEMS

Uptime is a critical consideration, particularly during difficult economic periods, since small missteps can have significant consequences and recovery from these problems is more difficult. Most top-tier hosted service providers offer very high levels of uptime (typically 99.9% or higher) and will typically offer Service Level Agreements (SLAs). This provides a level of service guarantee typically unavailable with on-premise deployments, and/or monetary payback if service levels are not met.

Built-in disaster recovery capabilities through redundant data centers can provide built-in business continuity as part of the basic offering. Deploying a second data center for an on-premise deployment would be cost prohibitive in most cases, particularly for smaller organizations.

MINIMAL VULNERABILITY TO SPIKES IN SPAM, NEW FORMS OF MALWARE AND OTHER THREATS

Hosted providers typically use multiple virus filters, multiple spam filters and a variety of other defense layers to protect their customers. While it is possible for on-premise deployments to offer this level of protection, the cost of doing so is typically prohibitive for all but the largest deployments. Because they are servicing large numbers of users, hosted providers can integrate best-of-breed solutions from multiple vendors – something that most organizations could not afford to do on their own.

EASIER AND FASTER TO ADD ADDITIONAL SERVICES

Most hosted providers offer easy, Web-based provisioning services for their customers. This allows an office manager or a part-time IT staff member to add or delete users, increase storage for users on demand and add new services, such as archiving, with minimal effort and usually in just minutes. To add capabilities for on-premise deployments is typically much more expensive and time-consuming because of the need to evaluate and procure hardware and software (or appliances), deploy and configure it, assign IT staff time to be trained/certified and manage the newly added infrastructure. Will your 2009 budget accommodate the costs to allow you to do this? Will you be able to add more people and cover the costs of their training?

What Should You Do?

UNDERSTAND YOUR CURRENT EMAIL MANAGEMENT COSTS

Osterman Research has found that the vast majority of organizations cannot accurately estimate the cost of providing messaging services to their users. Further, we have found that many decision makers underestimate the cost of providing services. This results in an

inability to accurately understand just how much email and the associated enhanced services cost to maintain.

What decision makers should do, first and foremost, is calculate the true cost of providing messaging capabilities. This includes the hardware, software, bandwidth, storage, labor and 3rd party vendor support that are devoted to maintaining email and related services, such as anti-virus, spam control, mobility and message archiving. Doing so will allow decision makers to understand their in-house costs so that they can accurately compare alternatives to in-house email management.

ESTIMATE WHAT YOUR COSTS WILL BE IN 2009, 2010, 2011...

Because email is here to stay, it is important to estimate your long-term costs of ownership. This includes the cost of upgrading servers and software, adding new security capabilities as threats become more sophisticated and more serious, increases in labor rates, and the like. Estimating long-term costs will allow an organization to understand how messaging costs are increasing over time and will help to make better-informed decisions about alternatives.

CONSIDER EVERYTHING YOU'LL NEED TO DO OVER THE NEXT TWO TO THREE YEARS

As a corollary exercise to estimating long term costs, lay out a plan for what your organization will need to add to the current messaging infrastructure over the long term. This might include adding new servers or appliances to deal with new messaging threats, adding archiving capabilities for some or all of your users, implementing disaster recovery or business continuity capabilities, deploying redundancy to maintain high availability, and adding a variety of new capabilities you might not have yet considered.

How much more value could you get out of your IT staff if they were working on initiatives that could provide your company with a real competitive advantage?

CONSIDER YOUR OPPORTUNITY COSTS

It is also important to consider the opportunity costs of not using a hosted provider, but instead employing internal IT staff to maintain email and related services. As part of this exercise, it is useful to ask two questions:

- How much value does your IT staff contribute to your bottom line when they manage your email infrastructure?
- How much more value could you get out of your IT staff if they were working on initiatives that could provide your company with a real competitive advantage?

Decision makers who seriously consider these questions might conclude that they could derive more value from their internal staff if they employed them for activities that provided more value to the organization or more competitive advantage.

EVALUATE WAYS OF REDUCING YOUR COSTS AND INCREASING YOUR EFFICIENCY

This is a particularly important question, especially during periods of belt-tightening and economic uncertainty. There are a variety of ways in which costs can be cut and internal processes made more efficient. Many organizations will find that using a hosted provider for email will do just that.

Sponsor of this White Paper

Founded in 1997, USA.NET is the recognized leader in the outsourced messaging and collaboration market. The company offers a wide range of hosted email, collaboration and security services that solve business requirements for companies of all sizes.

USA.NET®

A Perimeter eSecurity™ Company

7900 E. Union Avenue

Suite 800

Denver, CO 80237

303.865.1223

800.653.0179

From its proprietary, Unix-based Commercial Messaging Service (CMS) platform, to its Hosted Exchange platform, USA.NET is the choice of SMBs and major enterprises alike because of its ability to customize each customer's solution. In addition to hosted email, USA.NET offers a suite of 50+ enhanced hosted services that address business concerns in areas such as spam, virus, collaboration, archiving, unified messaging, wireless messaging and network security.

With over 11 years experience USA.NET serves customers in 120 countries, processes over 38M emails per day and manages over 80 Terabytes of data. USA.NET is based in Denver, Colorado and is a wholly-owned subsidiary of Perimeter eSecurity in Milford, Connecticut.

Summary

Difficult economic times require organizations to more carefully consider their costs of doing business, particularly for those activities that cannot be eliminated. Because email is such a critical part of most organizations' business processes, it must be maintained as reliably and as cost effectively as possible. However, increasing threat levels, the need to add more capabilities to email, and increasing labor costs all contribute to a scenario in which internally managed email systems will become more expensive over time.

As a result, many organizations should consider using a hosted email provider. Doing so can result in more predictable and lower costs, improved protection from threats, provide a long-term roadmap for the provision of new services, and the ability to redeploy IT staff members to projects and initiatives that will provide greater value to the organization and could give it a competitive advantage.

© 2008 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.