

# The Growing Importance of E-Mail Continuity



an Osterman Research white paper  
sponsored by

**Microsoft®**

## Executive Summary

---

It sounds almost trite to call e-mail the killer app for most organizations. That said, e-mail truly has become the primary communications medium for most organizations, and it is the communications tool that users can least afford to be without.

Because corporate e-mail is used at all times—during normal business hours, when employees are at home, or by employees in multiple time zones—e-mail must remain continually available, whether at 10:00 A.M. on a Wednesday morning or at 11:00 P.M. on a Saturday night. An e-mail downtime of even 30 minutes can carry with it serious ramifications for employee productivity and corporate revenue, not to mention downtime incidents that can last days or weeks because of hurricanes, floods, or other natural disasters.

In short, e-mail must remain continually available because business must remain continually available. This white paper examines the issues surrounding continuous e-mail availability and discusses a solution to address the need to make e-mail available around the clock.

## Why Consider E-Mail Continuity?

---

Clearly, e-mail is the single most critical application that organizations operate. E-mail is the primary file transport mechanism in use by most organizations. It is more important than the telephone for most users, it increasingly is used as a repository of critical business information, and four out of five organizations use e-mail for conducting business transactions such as sending contracts or purchase orders. Further, because of the increasing use of attachments, the growing sophistication of these attachments, and greater use of e-mail in general, message stores are growing at more than 30 percent annually. In short, a critical business tool is becoming even more critical over time.

### ***E-mail is susceptible to major disruptions***

While e-mail is critical to the operation of almost all organizations, it is also susceptible to a variety of serious disruptions that range from leaky sprinkler pipes above e-mail servers to hurricanes. The string of hurricanes that hit the southern United States in 2004 and 2005, for example, caused widespread e-mail outages from which many organizations have yet to recover. Major power blackouts,

*An e-mail outage of even 30 minutes can carry with it serious ramifications for employee productivity and corporate revenue, not to mention downtime incidents that can last days or weeks because of hurricanes, floods, or other natural disasters.*

earthquakes, floods, ice storms, and other calamities can also bring e-mail systems down for days, weeks, or months at a time. Building closures due to bomb scares, terrorist threats, and other potential problems can also bring e-mail systems to a grinding halt. A company with offices near any federal facility, for example, can be shut down at a moment's notice based on just the potential for a terrorist attack.

*While major disasters can have an enormous impact on e-mail system continuity, it is usually the minor disasters that have the greatest impact on e-mail continuity because of their much greater frequency and their inability to be predicted.*

### **E-mail is also susceptible to minor disruptions**

While major disasters can have an enormous impact on e-mail system continuity, it is usually the minor disasters that have the greatest impact on e-mail continuity because of their much greater frequency and their inability to be predicted.

Organizations must contend on a regular basis with unplanned downtime incidents owing to server hardware crashes, software bugs, power surges, burst water pipes, operator mistakes, and a host of other relatively minor problems. Osterman Research has found that the typical organization experiences a median of 18 minutes of unplanned downtime during the typical month, but that one in five organizations experiences more than one hour of unplanned downtime each month.

Add to this the planned downtime that organizations encounter for activities like server maintenance, patch management, upgrades, migrations, and other normal maintenance. Osterman Research has found that the typical organization intentionally brings down their e-mail system for a median of 50 minutes each month, but that more than one-third of organizations experience more than one hour of planned downtime each month.

Further complicating the issue for e-mail managers trying to maintain e-mail system continuity are factors that are completely outside of their control, such as telecommunications or wide-area network problems that can bring e-mail systems down just as quickly as internal problems.

### **Disruptions in e-mail continuity can have significant impacts**

Because e-mail has become so critical to organizations of all sizes, even very short disruptions in e-mail continuity can have a serious impact on employee productivity. Studies have shown that when e-mail is unavailable, users who rely on it for their normal day-to-day workflow are significantly less productive during the outage. For example, if we

assume that an e-mail user is 25 percent less productive when e-mail is unavailable, and if that user's fully burdened salary is \$65,000 annually, then every hour of downtime for a 1,000-user organization will cost more than \$7,800 in lost employee productivity.

*E-mail downtime can create serious problems for an organization's reputation. E-mail that bounces back to senders can, at best, be annoying for potential customers or business partners; at worst, it can create the impression that an organization is no longer in business.*

Even more serious, however, are the negative impacts that e-mail downtime can have on corporate revenues. Because e-mail is increasingly used for critical business processes—including revenue-generating activities like accepting orders and sending time-sensitive proposals—even very short e-mail disruptions can have serious consequences for an organization's bottom line. An organization that receives orders through e-mail, for example, can experience revenue loss in the tens of thousands of dollars per hour when e-mail is unavailable.

### **Reputation can suffer from e-mail downtime**

E-mail downtime can create serious problems for an organization's reputation. E-mail that bounces back to senders can, at best, be annoying for potential customers or business partners; at worst, it can create the impression that an organization is no longer in business.

## **Why Messaging Continuity Provides Value to an Organization**

---

Because of the serious ramifications that e-mail downtime can have, it is critical for organizations that rely on e-mail to have a backup capability that can maintain the continuity of e-mail during planned and unplanned downtimes. Any such capability should have the following characteristics:

- It should be available at all times as a hot standby e-mail system to handle any length of disruption, whether the disruption lasts a few minutes or several weeks.
- Because the vast majority of e-mail users periodically refer to past e-mail content when composing new messages, e-mail from the recent past should be available to users for reference purposes in the backup system.

Also, the standby system should be available as a backup system so that IT staff can maintain e-mail continuity during scheduled e-mail outages, such as during system upgrades or when migrating users to a new system. Because users often need to access their e-mail during these planned

outages, a standby e-mail system should be available to manage user demands for e-mail access during planned outages.

Perhaps most importantly, a standby e-mail system should insulate the outside world from any and all internal e-mail disruptions, whatever their cause. By maintaining 100 percent availability to e-mail, an organization can ensure that its most critical communications asset is always available to internal users and to external users.

*A standby e-mail system should insulate the outside world from any and all internal e-mail disruptions, whatever their cause. By maintaining 100 percent availability to e-mail, an organization can ensure that its most critical communications asset is always available to internal users and to external users.*

### **Options for Making Messaging Continually Available**

There are basically three options to consider for an organization that realizes its need to implement a backup e-mail system:

- **Provide consumer Webmail accounts to all e-mail users**  
The least expensive option is simply to provide all users with their own consumer Webmail accounts, such as Hotmail or Yahoo! Mail. While this approach allows users to maintain access to e-mail and is very inexpensive, this approach has some serious shortcomings. The corporate domain still remains unavailable during a system outage, so e-mail sent to users' primary e-mail accounts continues to bounce. Users do not have a historical record of their e-mail from the recent past. A corporate directory is unavailable, so users cannot communicate with each other unless they share personal Webmail addresses among themselves. The Webmail option provides no control for the corporate e-mail administrator over policy violations. Plus, this approach is the least professional of the three options discussed here because the corporate domain is not used in e-mail. In short, personal Webmail accounts are an inexpensive, but inadequate option for virtually all organizations.
- **Deploy a fully redundant e-mail system at a remote location**  
This option is a viable one because it allows the primary corporate domain to continue operating during a failure of the primary e-mail system. It provides users with access to their historical e-mail, assuming that a capability has been implemented to replicate data between the primary and backup e-mail systems in real time. Plus, users can continue to operate more or less normally with only a slight modification to their accounts to point their

e-mail clients to the backup servers during a failure of the primary system.

This option is very expensive, however, because a fully redundant system, including the labor to manage it, must be maintained at a remote facility on a continuous basis. Based on Osterman Research cost estimates, the cost to acquire and maintain a primary messaging system for three years is approximately \$25 per user per month. A complete backup e-mail system roughly doubles this cost, making it a poor option for most organizations. Plus, this approach uses valuable IT staff time that could otherwise be put to more productive uses.

*A hosted solution for e-mail backup provides all of the benefits associated with an internally managed backup e-mail system, but at significantly lower cost.*

- **Use a hosted solution**

A third option—one that provides the advantages of low cost per user with the ability to continue to use the corporate domain—is a hosted solution. A hosted solution for e-mail backup provides all of the benefits associated with an internally managed backup e-mail system, but at significantly lower cost. A hosted solution reduces the necessary IT staff investment to manage and integrate with the primary e-mail system and can be activated within minutes of a failure in the primary e-mail system. Messages to the corporate domain will not bounce, allowing continuity of message flow among customers, prospects, partners, and others. Plus, users have access to historical e-mail so that they can review and respond to older e-mail when composing new e-mail—something that the vast majority of employees do. Plus, users' e-mail addresses don't change, so all employees have access to contact information for everyone else in the company. Just as importantly, such a system is available at any time and for any reason that the primary e-mail system goes down—even if it's just for maintenance purposes or temporary glitches of a mail server in the wee hours of the night.

### **Why Messaging Backup Must Always Be Available**

Regardless of which option an organization chooses to provide e-mail continuity in the event their primary e-mail system fails, such a capability must be available at a moment's notice because a failure of the primary e-mail system typically occurs without warning due to unpredictable events like a power blackout, a server crash, or a fire. As a result, such a system must always be on, ready for cutover immediately in order to maintain e-mail continuity.

While consumer Webmail accounts that serve as backups for primary e-mail accounts are generally quite reliable, they carry with them the significant disadvantages noted above. An internally managed, redundant e-mail system can also provide immediate availability and a variety of other benefits, but it is expensive to deploy and maintain and it must be staffed around the clock, adding to the already significant cost of this approach. A hosted solution is always available. It provides many more advantages than consumer Webmail accounts that are used for backup, and it is dramatically less expensive than an internally managed solution.

*A hosted solution is always available. It provides many more advantages than consumer Webmail accounts that are used for backup, and it is dramatically less expensive than an internally managed solution.*

## Examples of E-Mail Continuity in Action

---

- **Example One: E-Mail Insurance with Microsoft Active Message Continuity**

2005 goes on record as one of the worst hurricane seasons of all time. In August 2005, Hurricane Katrina devastated the city of New Orleans. Storm surges destroyed the levees that protected the city's perimeter. Two weeks later, Hurricane Rita set a similar course for the city of Houston, and businesses scrambled to ensure that similar devastation did not befall them.

An architecture and construction firm, headquartered in Houston, relied upon e-mail to share design plans and contract status among its 515 employees across the United States. Its e-mail infrastructure was housed in Houston, and the firm knew that damage from a hurricane had the potential to grind its business activities across the United States to a halt. The firm turned to Microsoft to implement an E-mail Continuity solution that would provide Web-based back up to e-mail in the event that its servers went down. Thankfully, hurricane damage wasn't as bad as predicted, but administrators at the firm had the peace of mind that business would continue even if a catastrophe occurred.

- **Example Two: Server Maintenance During Business Hours**

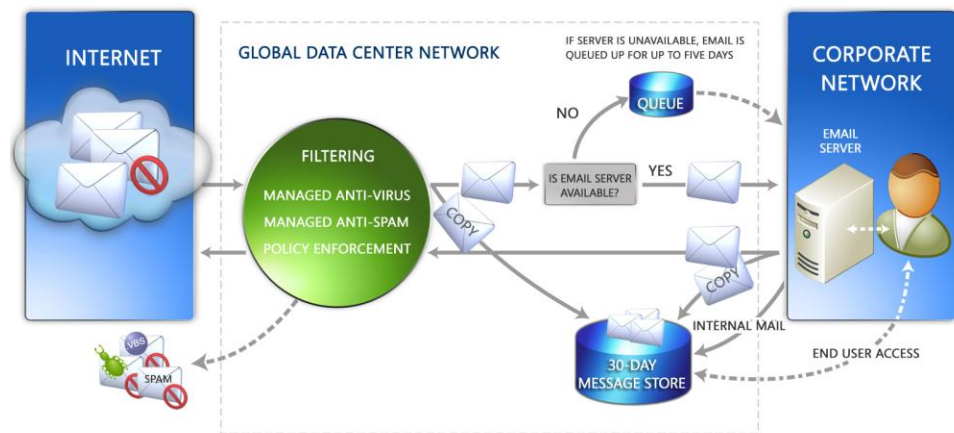
One of the most powerful law firms in Los Angeles uses Microsoft Exchange Hosted Continuity to provide attorneys with access to e-mail even during scheduled server maintenance. Time is literally money to this firm, and every second of downtime translates into a missed opportunity to provide billable counsel to clients. Now, in the event of a server outage, attorneys turn to the Web-

based interface for continuous access to e-mail functionality.

## An Overview of Microsoft Exchange Hosted Continuity

Exchange Hosted Continuity is an always-on, e-mail continuity and disaster recovery service. The service ensures that a business's employees have continuous access to e-mail even during disaster and emergency situations. Exchange Hosted Continuity makes copies of inbound, outbound, and internal e-mail instream, and then stores those message copies in a rolling 30-day message store. E-mail administrators and end users can access the message store at any time to recover messages that may have been lost or deleted from an enterprise's primary e-mail environment.

*Exchange Hosted Continuity is an always-on, e-mail continuity and disaster recovery service. The service ensures that a business's employees have continuous access to e-mail even during disaster and emergency situations.*



**Figure 1: Exchange Hosted Continuity operates in concert with Microsoft Exchange Hosted Filtering to filter unwanted e-mail content from the mail stream. In an emergency, users are assured access to 30 days of true business e-mail.**

The service's Web-based interface includes e-mail tools for composing, reading, and replying to e-mail, ensuring continuous access to all e-mail functionality even when the primary e-mail environment is unavailable or a backup e-mail system is needed. Any messages sent by means of the Web-based tools can be merged into the primary mail system to complete disaster recovery operations.

If the primary mail environment is down or a business's network is unavailable, Exchange Hosted Continuity continues to copy messages to the message store and queues the original message for delivery once the primary e-mail environment is restored.

## Feature Summary

---

*If the primary mail environment is down or a business's network is unavailable, Exchange Hosted Continuity continues to copy messages to the message store and queues the original message for delivery once the primary e-mail environment is restored.*

- E-mail continuity and disaster recovery delivered as a managed service with 30-day message storage.
- Instream message capture for inbound and outbound e-mail; internal e-mail captured through the journaling function of the primary e-mail server.
- Web-based access to message store and e-mail tools for end users and administrators.
- Web-based interface allows for composing, reading, forwarding, restoring, and replying to e-mail.
- Ability to configure roles and access privileges; global and individual settings.
- Event log to track and audit system activity.
- Call tree lists for notifying staff in the event of an outage.
- Message restoration after outage.
- Global password reset for users in the event of an emergency.
- Searchable message store; users can search message header; retrieve and restore searched messages.
- Summary and drill-down e-mail traffic reports can be scheduled and delivered through e-mail.

## Conclusion

---

E-mail is the most critical communications asset for organizations large and small. As such, e-mail must remain available on a continuous basis and must be immune from downtime-inducing problems ranging from server crashes to hurricanes. Organizations should implement a backup e-mail system that serves as an always-ready hot standby that can be employed during outages of the primary e-mail system. Making such a system available ensures that productivity, revenues, and corporate reputation are maintained.

## About Microsoft Exchange Hosted Services

---

Microsoft Exchange Hosted Services offer a cost-effective way for enterprises to actively ensure the security and availability of their messaging environment, while instilling confidence that their messaging processes satisfy internal policy and regulatory compliance requirements. A seamless extension of Microsoft Exchange that operates over the Internet as a service, the complete line of services includes hosted filtering for spam and virus protection; hosted archiving to satisfy compliance requirements and internal policies; hosted encryption to preserve e-mail confidentiality; and, hosted continuity for ongoing access to e-mail during and after disasters. Microsoft Exchange Hosted Services provide value to corporate customers by eliminating upfront capital investment, freeing up IT resources, and removing incoming e-mail threats before they reach the corporate firewall.

For more information, visit

<http://www.microsoft.com/exchange/services>

*Organizations should implement a backup e-mail system that serves as an always-ready hot standby that can be employed during outages of the primary e-mail system. Making such a system available ensures that productivity, revenues, and corporate reputation are maintained.*

© 2006 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 by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.