A MIMECAST SPONSORED WHITE PAPER

EMAIL AS PART OF A BUSINESS CONTINUITY STRATEGY

WHY ALWAYS-ON-BUSINESS REQUIRES ALWAYS-ON-EMAIL

Few businesses could function without email, and email provides a critical coordination tool during an outage, yet due to the cost and complexity of providing true email continuity many businesses do not have business continuity plans that protect email adequately. Continuity and archiving services may prove more cost effective for email than high-availability clustering, especially when considered in the light of continued governance, risk mitigation and compliance.

CONTENTS

AUDIENCE AND REMIT

The intended audience for this White Paper includes those concerned with creating or implementing email management strategies, as well as managers with responsibility for business continuity processes. The paper looks at the general approaches available to ensure email continuity from a high level and the implications of deploying each strategy on infrastructure, budget, people and resilience.

MIMECAST FOREWORD

Email is one of the most critical applications in use in business today: it is embedded in many business workflows, it is used by engineers to inform them of infrastructure issues and it is used to communicate with customers and business partners. In short, the modern organization has email at the heart of its communications and business processes. This makes it critical to minimize both the downtime and loss of email upon the outset of a business continuity event.

Maintaining email is no longer about keeping just the mail server itself online, organizations now employ email infrastructures containing multiple products to mitigate the risk of malware, spam, litigation and non-compliance.

Maintaining access to email while upholding risk mitigation and compliance is a challenging endeavor, this white paper discusses the issues involved with addressing this problem.

EXECUTIVE SUMMARY

Email has become an integral part of business and it’s crucial to include it in business continuity planning. It’s inevitable that email systems will fail and the business can assess the risks and provision systems to avoid the costs of lengthy email outages.

But traditional approaches to availability and recovery may not offer adequate protection for email systems at an affordable price, especially as it is now often a legal obligation as well as a business necessity to ensure that no messages are lost. Indeed, email is particularly important during a disaster, when staff will need to keep in touch more urgently than usual; they will also be under more stress so providing a transparent and familiar system is key.

Invoking a business continuity plan is expensive and therefore reserved for significant disasters. To this end a service-based email continuity solution may well be the best approach for both reliability and cost. Having an email continuity solution that can be invoked at minimal cost and with minimal disruption provides the additional benefit of providing flexibility in the patching and upgrading of the email server.

BUSINESS CONTINUITY PLANNING AND EMAIL

More mobile workers, more demanding customers, global competition, the increasing need for business agility, sheer convenience; there's a range of reasons why email has become so important for modern business. The vast majority of decision makers rate email as a mission-critical business resource for communicating and transferring files; email remains the preferred business communications channel for 93% of enterprise users[1], most information workers rely on email more than even the telephone[2] and up to 60% of business-critical data is stored in email[3].

Email is business critical

Email isn't just a list of messages. It's purchase orders, contracts, proposals, enquiries, customer orders, business documents and discussions. Email is the way nearly every business makes decisions and gets work done, complete with the context of how and why those decisions were made, stored in a way humans can make sense of intuitively. But email servers were designed for delivering messages rather than managing and storing them. They don't have the storage capacity or search tools that users want, they don't have the administration and reporting tools that IT departments and managers need and like any other IT system they're subject to viruses, power outages, natural disasters, corruption, human error and media failures.

If the mail system fails, the results range from lost productivity to losing orders and customers; from fines and litigation to business failure within a surprisingly short period of time[4]. Therefore making sure that email stays available is a key part of any business continuity plan. However only a third of businesses would be able to continue using email without any interruption or data loss in the event of server failure. Nearly as many (29%) have no contingency plans and would have to resort to private email addresses and phone calls or simply send employees home[5].

Getting the business back online

Business continuity involves much more than just disaster recovery. If a business is to be able to take any disaster in its stride, it needs to be able to operate during the recovery process, and provide tools to deliver key business services without full access to central business systems. A Business Continuity Plan (BCP) is an important tool for any organization as it allows recovery coordinators to identify key processes and people. The resulting plan will bring these people and processes online as soon as possible after any major incident in order to ensure that the business can communicate with customers and staff. A BCP also allows a business to test its continuity approach, with targets that must be met.

Business continuity involves much more than just disaster recovery.

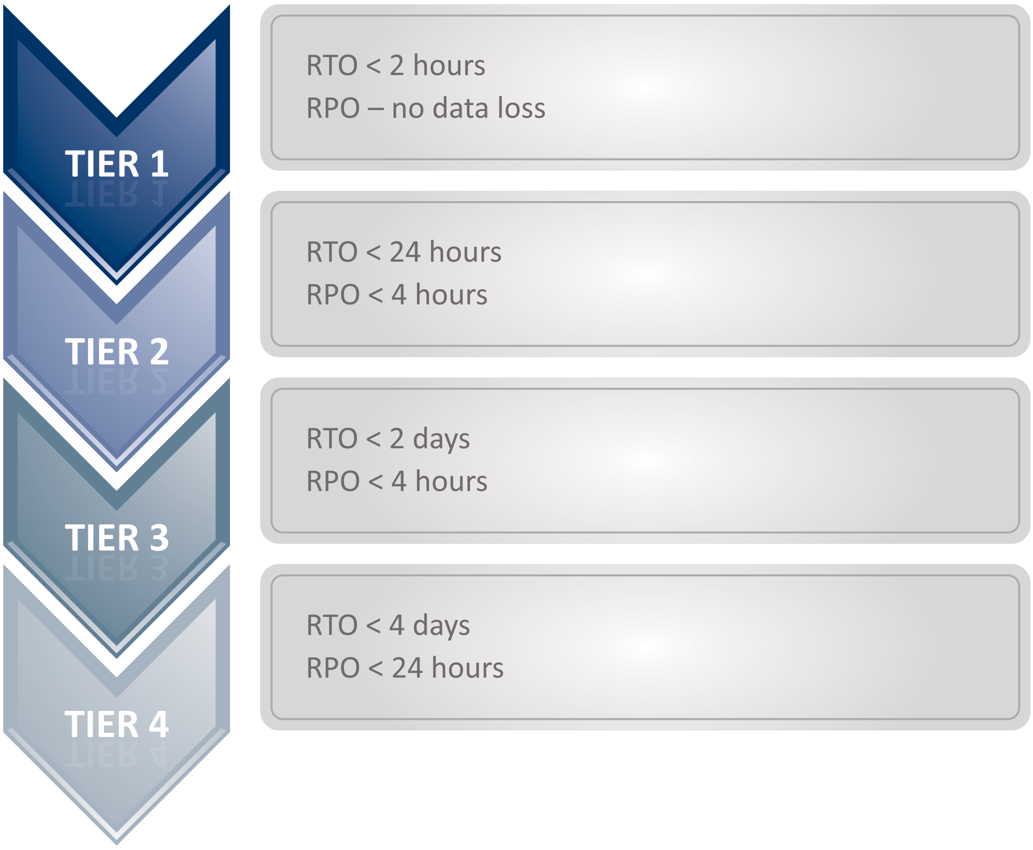
Recovery objectives

As a first step towards recovery, systems supporting critical business processes need to be prioritized. The time to bring the service back online is known as the Recovery Time Objective (RTO). The RTO needs to be as low as possible for key processes – preferably zero, assuming the cost is realistic. Recovery processes and systems should be available at all times, so staff can switch to them as quickly as possible. The business also needs to have access to all process-sensitive data, so that users can communicate effectively with customers and the rest of the business staff. This means that all recovery systems would ideally have a zero Recovery Point Objective (RPO) so no data is lost.

Email – a critical component of a BCP

Email is a critical component of a BCP for the majority of businesses. It's at the heart of ad hoc knowledge management networks, and a key customer communication channel for sales and marketing. This makes email a critical business tool – but it's one that is often overlooked in continuity planning.By making email a critical component of any BCP, with a low RPO and a low RTO, a business can keep operating with minimal impact on customer perceptions. A low RPO is essential, as information stored in archived email messages is key to providing the context manual business processes require. If email systems have too high an RPO, the ability to process orders and customer information – or actual data – could be lost during the recovery process.

RTO AND RPO TIMES FOR DIFFERENT TIERS OF BUSINESS APPLICATIONS



TIER 1
RTO < 2 hours
RPO – no data loss

TIER 2
RTO < 24 hours
RPO < 4 hours

TIER 3
RTO < 2 days
RPO < 4 hours

TIER 4
RTO < 4 days
RPO < 24 hours

FIgure 1:
Email should be treated as a tier 1 application based on its importance to businesses today.

A consistent flow of information during outages

Email can also be used to inform users of the continuity situation, though in practice it is best to keep it operating as normal. Using information held in email systems maintains the flow of backup business processes as well as consistent contact with customers.

A business needs email even more for delivering information to internal users when faced with disaster recovery. A low RTO means that email systems can be used to inform staff of the business situation, and to brief staff on how to respond to customers. With staff dispersed to recovery locations or working from home, perhaps even using personal machines, secure access to email means that backup business processes can be run effectively in a temporarily distributed organization.

Information stored in email can be accessed from anywhere – unlike information in desktop machines which may be unavailable, or even a total loss.

The key is to use email to focus on the business, not on recovery. Dedicated resources will be handling recovery – the rest of the business needs to continue operating as near normally as possible. A normal flow of communications during a disaster situation can be very reassuring to staff who may be working under considerable stress.

AVAILABILITY, RECOVERY AND CONTINUITY

Traditional disaster recovery methods have concentrated on ensuring system availability and data recovery. Availability is intended to ensure that systems never fail or that the possibility of failure is reduced. Recovery strategies aim to ensure that if and when something does go wrong, systems can be recovered and services restored, though the timescales can be unacceptable.

Continuity strategies provide access to services during a system failure via an independent infrastructure, usually offsite. This approach reduces the downtime risks associated with availability and recovery, and needs to be considered where maintaining business processes is a critical part of a BCP.

MOST APPROPRIATE STRATEGIES BASED ON COVERAGE IN EVENT OF SYSTEM FAILURE

Causes of failure	Availability	Recovery	Continuity
Mail server hardware failure	✓	✓	✓
Mail server software/OS failure		✓	✓
Mail server database corruption		✓	✓
Mail server backup file corruption			✓
Operator error		✓	✓
Power outage	✓		✓
Local network failure	✓		✓
Internet connectivity failure			✓
Physical disaster (flood, fire)		✓	✓

Figure 2:
A continuity strategy overcomes the shortcomings of availability and recovery strategies.

Building highly available systems

Redundant and resilient infrastructure like Redundant Array of Independent Disks (RAID) storage, redundant network topologies and clusters on the same site improve availability. In principle the level of protection will increase with the cost of the systems – which can be significant – but this still leaves the main site as a point of failure. In practice, it's impossible to protect against all hardware and software failures, so backup technologies and offsite solutions are required to provide recovery options.

Unless backups are made continuously, there will inevitably be some data loss and therefore a higher RPO. Reducing the length of RTO and the impact of RPO increase the cost of the backup solution through additional hardware, the facilities required at the alternate location and the infrastructure for real-time replication. Tape backup is the cheapest solution and online backup is convenient but in either case the recovery time can be hours or days and data can only be recovered from point of the last working backup.

Recovery plan basics

During a business continuity event, recovering data is only part of the story; servers and applications may also need to be rebuilt and reconfigured. Even virtual machines will need to be provisioned. If changes to the mail system mean configuration changes for email clients (especially on mobile devices), it's important to factor in the time to make these changes and how you will convey the information to remote staff in the absence of email.

The speed with which an alternative site can be operational is directly linked to cost. A 'cold' site has air-conditioning, electricity and telecoms but no hardware on site and no data replication. 'Cold' sites are the cheapest option but it can take weeks to have hardware delivered and set up and offsite backup tapes retrieved and delivered.

A 'warm' site with partially redundant hardware and software and regular replication will be able to take over some business functions within hours or days, but it will usually be necessary to obtain and restore backups to supplement the most recent replication. This is significantly more expensive, but still cheaper than a 'hot' site with fully redundant hardware and software that can take over all primary site operations within minutes or hours (although again, offsite backups may need to be obtained and restored). The continuous replication to a 'hot' site reduces the RPO to close to zero; having clustered standby mail servers reduces the RTO. Both increase the costs for the site and for the network infrastructure to support replication.

COST AND RECOVERY OBJECTIVES OF DIFFERENT EMAIL RECOVERY OPTIONS

	Restore on cold site	Continuity via remote SaaS email backup service	Replication to warm site	Log shipping with transaction level replication to remote datacenter	Asynchronous replication to hot site	Offsite high availability cluster with standby mail servers
Replication	None	Continuous	Daily or weekly	Minutes to hours	Daily or hourly	Continuous
RTO	Weeks	Failover within seconds	Hours to days	> 2 hours	> Minutes to 2 hours	Immediate failover
RPO	To last backup	No data loss	To last replication/ backup	To last replication	To last replication	Minimal data loss
Cost	Cheapest					Most expensive

Figure 3:
Organizations should aim for the lowest Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) balanced against the cost of implementation.

THE HUMAN SIDE OF CONTINUITY

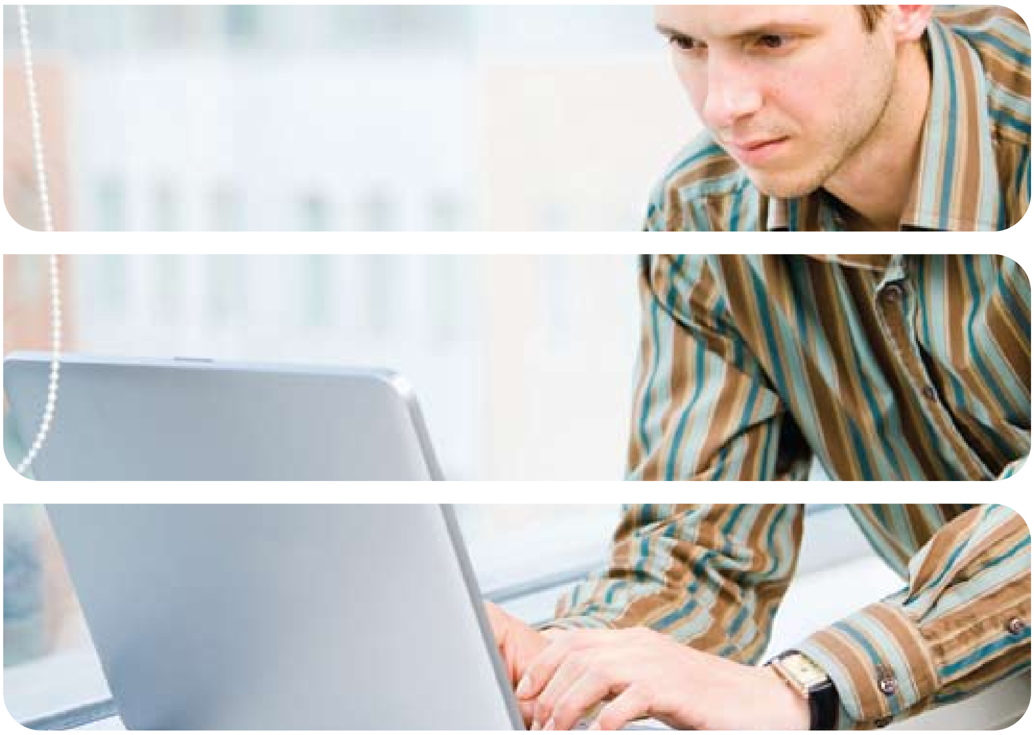
The technology isn't the only thing to consider. It's only natural that a disaster affecting a business will also affect its staff. Initial shock will reduce staff effectiveness, and businesses should be prepared to see an increase in person-to-person communication as staff members seek to come up with a common response to events, and to use internal informal communication channels to get additional information above and beyond that provided by management. Email is a key part of this.

Preparing your employees

In the event of an outage, providing instructions and open access to information will help employees. Once staff members have made initial adjustments to the interruption in service there will still be decreased efficiency, as backup manual processes described in a BCP will be unfamiliar at first. This unfamiliarity will also increase the risk profile of the business, as unfamiliar users are more likely to make critical mistakes. Processes should be designed to reduce this risk as much as possible.

Transparent continuity environment

Low RTO and RPO are important in minimizing business risk, as well as the ability to use familiar tools and systems – even at home or at a continuity location. There is also a need for businesses to be transparent about their BCP, and about the tools and information that will be available in the event of significant business system failures. Users who are familiar with their roles during a crisis will respond more effectively, reducing business risk significantly. A seamless transition to a continuity environment will also help, especially if users are able to use familiar email tools – both on the desktop and mobile devices.



THE BUSINESS CONTEXT OF CONTINUITY

Businesses need to operate in compliance with the current regulatory environment – and that doesn't go away even if a business suffers a major outage. An effective business continuity plan needs to consider regulatory requirements, and will need to describe the governance and risk management process that will apply while the plan is in operation. Whether it's a fire, a flood, or any other disaster, the regulators will expect a business to continue operating in a compliant manner which is much harder without familiar systems and under stress. Business systems, including email, are key to managing risk and maintaining governance and compliance; continuity needs to be considered in the context of these business demands.

Reducing risk

A sound approach to Governance, Risk and Compliance (GRC) pays dividends during normal operations and disasters alike, according to the annual report of the IT Policy Compliance Group[6]. "The way to improve business results and reduce financial risk, loss and expense is to increase or enhance the competencies, practices and capabilities governing the use and disposition of IT resources." The correlation between business success and sound IT GRC policies is clear[7]: "Organizations with best business results are the same firms with the most mature practices and the organizations with the worst business results are the same firms with the least mature practices."

Governance and compliance

A well designed BCP will include GRC elements, and will use them to minimize business risks. A virus outbreak or social engineering attack is much more likely to be successful during the stress of a disaster and when ancillary services that support email, such as malware protection, are not considered within the BCP plan. In addition, having to work around failing systems can put data security and customer privacy at risk. Having these elements in place will ensure management doesn't have to explain to the Information Commissioner that customer privacy wasn't seen as a critical function, or to the Financial Services Authority that transaction transparency was deemed unnecessary because of the emergency.

Effective governance during business continuity operations isn't just about regulatory compliance. It's also a tool to help businesses cope with any legal fallout from effects of its continuity operations. Disasters can mean delayed deliveries, missed deadlines or lost documentation, which will mean customer complaints or in the worst case, legal action. Contractual obligations need to be met, and if this is impossible, then all actions need to be documented – especially any that show the business did its best to mitigate risks to its customers and that it operated according to best practices and with due care. A well-designed continuity plan will include this as part of any risk management process.

COST, COMPLEXITY AND CONTINUITY

Backup systems, availability and recovery are all necessary, but to keep business systems going at an affordable cost businesses need to ensure continuity for key systems, including email. Email continuity isn't just about the mail server either; modern email environments are multi-faceted so continuity has to cover archiving and data protection, security options like anti-spam, anti-virus and anti-phishing tools, any systems needed for mobile email and all the other support services. While clustering and a 'hot' standby site provide true high availability and the best experience for end users, the cost and complexity of protecting the wider email environment this way can be prohibitive.

Effective continuity requires simplicity. Complex, fragmented email environments are hard to manage effectively – and harder still to turn into systems that can survive a disaster or a major outage. The need for simplicity goes beyond the demands of business continuity, as simple systems are easier to handle with governance, risk management and compliance policies and procedures. With well-designed email systems and a complete BCP, it's possible to manage continuity so that existing policy enforcement, security tools and retention procedures remain in place – while keeping costs to a minimum.

ACHIEVING ZERO DOWNTIME

According to Gartner, email uptime is the single most critical email SLA metric. There are two main alternative methods for achieving that as one of the aims of a business continuity plan and keeping a business ‘always on’ by providing a highly-available messaging infrastructure.

Option 1:

Build a ‘hot’ site

A ‘hot’ site can take over in minutes or seconds but the initial investment of hardware, software, and datacenter costs to create a fully redundant site will quickly add up. Building, maintaining and upgrading this site will also be a time-consuming task for even the most well equipped IT departments.

Option 2:

Connect to a continuity service

Connecting to a continuity service can eliminate upfront costs as continuity services do not typically require hardware or software investments. Additionally, the IT department, although still in control of the service, is relieved of the complex planning and intensive administrative tasks involved in upgrading and maintaining infrastructure. These low-cost subscription-based services have a low barrier to entry, can be provisioned in hours and provide a comprehensive and flexible solution to today’s messaging business continuity challenges, thereby helping to simplify governance and risk management requirements.

MIMECAST CONTINUITY SERVICE

Mimecast provides a complete email lifecycle management solution that also offers an email continuity service.

By integrating security, policy, retention and discovery services through a single management and reporting interface, customers can get an instant snapshot of their most critical communications platform.

Historical messages are available instantly and in the event of a failure on the main site, email service can failover seamlessly with no loss of data. The service supports minimal recovery time at the time of failure and when the business switches back to in-house mail servers.

The Mimecast offering is a Software-as-a-Service that can be deployed in hours, providing a unified email management service that can replace dozens of independent point solutions related to hygiene, policy, continuity, retention and discovery.

REFERENCES

1. EIU: The digital company 2013: How technology will empower the customer http://www.eiu.com/site_info.asp?info_name=2013&page=noads

2. Osterman Research: A Guide to Understanding Hosted and Managed Messaging, August 2007 http://i.i.com.com/cnwk.1d/html/itp/Google_A_Guide_to_Hosted_and_Managed_Messaging_FINAL.pdf

3. Gartner: Establishing Email Service-level Agreements, July 2007

4. Contingency Planning and Management Magazine (http://www.contingencyplanning.com): 40% of companies that shut down for 3 days failed within 36 months

5. Independent survey by emedia for Mimecast, August 2008

6. IT Policy Compliance Group 2008 annual report: IT Governance, Risk and Compliance – Improving business results and mitigating financial risk http://www.itpolicycompliance.com/research_reports/

7. IT Policy Compliance Group 2008 annual report: Profits, revenue and retention rates are higher, spending on regulatory audits is lower and the risks of loss or theft of customer data are 96% lower.

ABOUT MIMECAST

Mimecast Services for Microsoft Exchange®, Outlook®, Windows Mobile® and Blackberry® provide enterprise-level email continuity, archiving and security for any size of company. ‘Unified Email Management’ requires no hardware or software, integrates with an organization’s existing IT, offers complete control to the IT administrator and takes just hours to set up.

Every day Mimecast takes care of millions of emails and documents for thousands of companies around the world. Founded in 2002, Mimecast has operations in North America, Europe, South Africa and Offshore.

mimecast
unified email management

North America
275 Grove Street,
Building 2, Suite 400,
Newton,
MA 02466
tel: 1 800 660 1194
email: **info@mimecast.com**

UK & Europe
2-8 Balfe Street,
Kings Cross,
London,
N1 9EG
tel: +44 (0)207 843 2300
email: **info@mimecast.com**

South Africa
Morningside Close Office Park,
Block G, 1st Floor 222 Rivonia Road,
Morningside
tel: 0861 114 063 (S.A. local)
tel: +27 (0)112 585 300 (intl)
email: **info@mimecast.co.za**

Offshore
The Powerhouse,
Queens Road,
St Helier,
Jersey, JE2 3AP
tel: +44 (0)1534 752300
email: **info@mimecast-offshore.com**

WWW.MIMECAST.COM

©2008 Mimecast. All rights reserved.