

GFI White Paper

Email continuity: Safeguard email communications 24/7

Email is a critical communications tool. Email downtime means a loss of productivity, possible compliance and regulatory issues related to data loss or even lost revenues. Minimizing email downtime is an increasingly important part of an organization's messaging infrastructure and its disaster prevention and recovery strategy.

Contents

Introduction.....	3
Outages and their impact on business.....	3
Overcoming email outages.....	3
Hosted email continuity: options.....	4
The benefits of a hosted email continuity service.....	4
What to look for in a hosted email continuity service.....	5
Conclusion.....	5

Introduction

Email has become deeply ingrained in business operations. Internal communications are often accomplished more by email than by phone or face-to-face meetings. Communications with external clients, vendors, partners and other business contacts are perhaps even more dependent on email. Calls and meetings are scheduled by email; decisions are made based on email correspondence; inquiries, proposals and contracts are sent by email; communications, both mundane and critically important, are handled by email more than any other medium.

Businesses have become so accustomed to using email that a few minutes of server downtime is enough to have employees and executives alike calling the help desk. While a minute or two of email server downtime is not catastrophic, no organization can function effectively if downtime increases to hours or days.

Risk management and business continuity planning exercises should include email uptime as a priority. Businesses must not confuse email continuity with email archiving or email backups. The latter are suitable and necessary for disaster recovery but not for providing continued and seamless use of email when hardware or software errors occur or when a more serious disaster strikes.

Outages and their impact on business

Email downtime and outages are a business reality. At some point, something will go wrong and businesses need to be ready. Computer hardware will eventually fail and occasionally fails prior to scheduled replacement. Email or operating system software may experience errors. Data can become corrupted. And external events, such as network problems, flooding and power cuts, do occur on rare occasions. Indeed, email outages are common. According to Osterman Research, email systems experience a 53-minute mean of unplanned downtime each month, or 10.6 hours each year. And there are numerous reasons why businesses need to consider the potential impact of email downtime:

- » **Reduced productivity** – Osterman estimates that employees become 25% less productive when their email system is down.
- » **Loss of business** – Companies that use email for transaction processing, sales orders, client requests, and other communications with customers are at most risk of losing orders or losing clients when email is unavailable.
- » **Compliance or regulatory risks** – If a business experiences hardware or software problems with its mail infrastructure, without sufficient safeguards, important emails could be lost. Organizations that must comply with regulations or laws related to electronic data may also face compliance issues from the loss of those messages.
- » **Reputation risk** – Businesses dealing with clients on a daily basis cannot afford to appear unprofessional. Requests for information that are not answered within a reasonable time-frame may negatively impact the image of that business in terms of its perceived competence, reliability and professionalism – important characteristics that every business needs to protect.

Overcoming email outages

The good news is that email outages can be easily mitigated, at nominal expense. Unfortunately, many businesses fail to distinguish between the concept of an email backup or an email archive solution and an email continuity solution.

While most organizations have a disaster recovery strategy in place, that strategy typically involves rebuilding hardware and/or software and recovering historical email data from a backup or archive solution. This is different from having continued access to email during an outage. How can a company continue its work in a seamless fashion during the hours or days it may take to rebuild its infrastructure in the event of hardware or software failure, or worse, a regional disaster?

What businesses need is a system or service that provides continuous email functionality, no matter the state of the customer's network, server or data. To ensure mail and business continuity that is not dependent on the customer's local network, organizations need an off-site service that allows them to continue their critical email communications – including the ability to access and respond to inbound messages received while their infrastructure is down.

Hosted email continuity: options

An externally hosted email continuity service allows an organization to avoid lost productivity, lost business and other consequences that arise from email outages. There are three services that fall under this general category:

- » **Queuing only** – Messages are spooled when undeliverable, typically when a mail server goes offline. Users do not have access to these messages until the server is back online, after which queued messages are delivered. Emails are not lost but productivity is greatly reduced. A queuing only solution is not a true continuity solution.
- » **Continuity via queuing and integrated mail service** – Messages are spooled when undeliverable and users have full access to them while their mail server is offline via a web-based mechanism independent of the customer's network. At that website, users can view and respond to queued messages and create new ones. When the mail server is back online, the service delivers any messages still in queue. No emails are lost and productivity is not affected. This is an effective email continuity solution that is easily implemented.
- » **Rolling continuity** – All messages are continually spooled, regardless of server status, and stored on disk for about a week or longer. If the customer's mail server goes offline or data becomes corrupted, an administrator can 'play back' a previous stream of email messages from any time over the last, say, 7 days. Typically, users would also have access to an integrated web-based mechanism to view messages, in the event the customer's mail infrastructure is not available. This is a sophisticated email continuity solution, although it can be expensive and/or complex to implement.

The use of a hosted email continuity service is important regardless of current email backup or email archiving solutions. Due to the risks of an on-premise solution falling prey to problems affecting a customer's mail server or local network, an externally hosted continuity service is the only viable option for assuring continued access to email functionality.

The benefits of a hosted email continuity service

A hosted email continuity service with integrated mail functionality provides businesses with numerous benefits, including:

- » No need to invest in new hardware or systems
- » Automatic and immediate continuity, requiring no action from the IT team during an outage
- » Employees can continue to work, accessing and replying to emails
- » No emails are lost
- » No compliance or regulatory issues for businesses required to keep copies of emails
- » No training or maintenance required for IT staff, freeing up their time for other tasks – especially during an outage
- » Peace of mind: In the event of an outage, pressures to solve the problem are reduced by having an interim solution in place. This reduces the risk of errors during the recovery process.

Thus, under any circumstances – ranging from a brief, planned mail server upgrade, to a major network outage caused by a natural disaster – the organization can maintain a high level of business continuity with minimal effort.

What to look for in a hosted email continuity service

Businesses seeking a hosted email continuity service should consider:

- » Implementation requirements for an organization's IT team
- » Whether the continuity service is automatically activated when an outage occurs
- » Support offered by the provider – hours of availability, email vs. phone support, level of expertise, etc.
- » Ease of use – simplicity of solutions, in particular for employees with minimal IT knowledge
- » Pricing model – cost should be substantially less than that of the mail infrastructure with no hidden charges
- » Distributed infrastructure – ensure messages are reliably stored in multiple geographic locations.

Conclusion

With email being such a critical communication tool, organizations cannot afford any downtime. For this reason, organizations must consider an email continuity service to guarantee 24/7 uptime and provide peace of mind in the event of system failure, scheduled mail server or network upgrades or natural disasters that render their mail infrastructure inaccessible.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit <http://www.gfi.com/contactus>

**Disclaimer**

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.