

GFI WHITE PAPER

Email Continuity – protecting your business against email downtime

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 of its disaster prevention and recovery strategy.

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 these days handled by email more than by any other medium.

Businesses have become so accustomed to using email that even a few minutes of server downtime is enough to have employees and executives quickly calling the helpdesk. 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 in time, something will go wrong and most businesses are caught unawares. 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 or power cuts are rare but history has shown that they do occur.

Indeed, email outages are common and according to Osterman Research, emails systems experience a mean of 53 minutes of unplanned downtime during a typical month or 10.6 hours over a period of a year. This is why businesses need to consider the potential impact of email downtime:

1. **Reduced productivity.** Osterman estimates that employees become 25% less productive when their email system is down.
2. **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.
3. **Compliance or regulatory risks.** If a business experiences hardware or software problems with its mail infrastructure, without sufficient safeguards, important emails could be lost. Those organizations that must comply with regulations or laws related to electronic data may also face compliance issues from the loss of those messages.
4. **Reputation risk.** Businesses dealing with clients on a daily basis can ill 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 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 of hardware and/or software, and recovering of historical email data from a backup or archive solution. This is different from having continued access to email during an outage. How should a company continue its work in a seamless fashion during the hours or even days that 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 regardless of what has happened to 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 email that has been sent to the company while their own infrastructure is down as well as the ability to respond to those emails.

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:

1. **Queuing only.** Messages are spooled when they cannot be delivered, typically when a mail server goes offline. Users do not have access to those messages until their mail server is back online, after which the queuing service delivers the queued messages. Emails are not lost; however, productivity is greatly reduced and a queuing only solution is not a true continuity solution.
2. **Continuity via queuing and integrated mail service.** In this case, messages are spooled when they cannot be delivered. Additionally, users have full access to those messages while their mail server is offline, via a web-based mechanism independent of the customer's network. At that web site, users can view those messages, respond to those 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 and can be implemented without undue complexity.
3. **Rolling continuity.** Instead of messages being spooled only when the server is down, all messages are continually spooled, and stored on disk for perhaps a week or longer. If the customer's mail server goes offline or certain 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 access those 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 what solution may be in place for email backup or email archiving. Due to the risks with an on-premise solution falling prey to the same problem 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 in the event of a problem with the customer's own infrastructure.

The benefits of a hosted email continuity service

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

1. No need to invest in new hardware or new systems.
2. Continuity is automatic and immediate, requiring no action from the IT team when an outage occurs.
3. Employees can continue to work, accessing and replying to emails.
4. No emails are lost.
5. Businesses required to keep copies of emails will have no compliance or regulatory issues.
6. IT staff do not need to invest time in training or maintenance, freeing up their time for other tasks, especially during an outage.
7. Peace of mind: Even in the event of an outage, pressures to solve the problem are reduced since an interim solution is 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:

1. The amount of investment necessary; a good hosted continuity solution should require minimal expense and minimal time to set up.
2. The service level agreement provided by the vendor.
3. How much ongoing work would be necessary for the organization's IT team, and whether the continuity service would need to be triggered when an outage occurs.
4. The level of support offered by the provider – hours of availability, email versus phone support, level of expertise, etc.
5. Ease of use – how simple the solution is for employees, in particular those with minimal IT knowledge.
6. Pricing model – costs for the continuity should be substantially less than the cost for the mail infrastructure, and should not have the risk of hidden charges.

7. Distributed infrastructure – make sure that the messages are stored in a reliable, geographically distributed fashion, so that the vendor can provide a highly reliable continuity service.

Conclusion

With email being such a critical communication tool, organizations can ill-afford any downtime. It is for this reason that organizations need to seriously consider some form of email continuity service – a service that guarantees 24/7 uptime and provides peace of mind in the event of systems failure, scheduled mail server or network upgrades or natural disasters that makes offices inaccessible.

© 2010. 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.