Email Security

Best Practices and Avoiding Downtime

How Does Your Solution Compare on 7 Critical Dimensions?

rackspace®

Table of Contents

rackspace®

A. Overview

Email is the lifeblood of an organization. It's the predominant way we communicate and get things done. For most employees, more time is spent using email than any other application. The average employee sends and receives 110 emails per day and spends approximately 2.5 hours using email every day.[1] Stating the obvious, email is a business-critical application. As such, the average organization devotes a substantial portion of IT resources to managing their email, keeping it secure, and ensuring it remains up and running. Organizations strive to do this as efficiently and effectively as possible, but with limited resources, security and downtime risks can be a very real threat.

The purpose of this whitepaper is twofold:

1. Provide you with a deeper understanding of the factors that can impact your current email solution's security risks and unplanned downtime (whether you are using on-premises Microsoft® Exchange Server, another in-house solution, "free" hosted email, or another third party hosted email provider).
2. Help you better compare and evaluate your current email solution and email security and risk of unplanned downtime, versus moving to a newer version of hosted Microsoft Exchange from Rackspace.®

This whitepaper will focus exclusively on the dimensions of security and downtime as these are the mission-critical factors considered when evaluating your existing business email solution versus moving to Rackspace. This paper is not meant to be a feature comparison of the various email solutions, but rather a discussion of the security and downtime issues you might be facing with your current solution.

Should you conclude that switching your current solution to Rackspace is right for your organization, we provide multiple options to meet your needs:

1. Hosted Microsoft Exchange
2. Dedicated Microsoft Exchange
3. Hybrid Exchange (Hosted Exchange and Hosted web-based email)

Details on each of these solutions are provided in the Appendix of this whitepaper.

B. Security Issues

Protecting your company from security threats is one of the top issues facing every IT department. The challenges are many as there are a number of different dimensions to security and threats are constantly evolving.

The recent InformationWeek 2014 Strategic Security Survey[2] drives home how much security is on the mind of today's organizations:

- ✔ "Managing the complexity of security" reclaimed the **No. 1 spot** among 10 challenges facing businesses
- ✔ **75%** say their organizations are as or more vulnerable to malicious code attacks and security breaches compared with a year ago
- ✔ **58%** see an infected personal device connecting to the corporate network as a top endpoint security concern
- ✔ **56%** say cyber-criminals pose the greatest threat to their organizations

Some of those same security concerns may raise questions for organizations that are considering moving email to the cloud. About 42% of companies have moved their email to the cloud (although another 22% expect to do so over the next year).[3] The reasons consistently center on concerns around data loss and security. There is an inherent assumption that it is more secure to remain on-premises versus moving to the cloud. But is this assumption warranted? Is your organization really more secure running your email on-premises versus in the cloud? Let's analyze the different security dimensions so you can see how your solution stacks up.

#1 Physical Security

While data security tends to be more focused on protection against viruses and malware, for many organizations, physical security should be an equal concern. Physical access to email servers and network equipment can create substantial security vulnerabilities. The ability to gain physical access to servers and network equipment enables information to be downloaded, or worse, can create an opening for hackers to access the entire network.

Physical access to your email servers should be controlled and limited to authorized personnel and a robust system of checks and balances should be in place.

PHYSICAL SECURITY BEST PRACTICES

Rackspace adheres to industry best practices across all of our global data centers.

- Data center access is limited to Rackspace data center technicians; every data center employee undergoes multiple and thorough background security checks before hired
- Biometric scanning controls data center access and provides an audit trail
- Security camera monitoring is employed at all data center locations
- 24x7x365 onsite staff provides additional protection against unauthorized entry
- Unmarked facilities help maintain a low profile
- Physical security is audited by an independent security consulting firm

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Does your organization have a robust system in place to ensure only authorized employees have access to your email servers (such as electronically controlled access tied to individual employees)?
2. Do you have the ability to control this access and audit individual employees?
3. Have you ever had an audit of your physical security policies and procedures?
4. Does your email provider incorporate security and privacy best practices in their data centers?

#2 Anti-Spam/Anti-Phishing

In the "best" case scenario, spam is merely a productivity drain on the organization. It wastes employees' time and needlessly clogs inboxes. In the worst case scenario, it delivers very harmful malware and viruses that can compromise security. It is estimated that spam represents 70% of all email traffic.[4]

Spammer tactics are constantly changing and evolving to avoid detection. New tactics arrive every month, with the latest examples being faked booking notices from airlines and fake virus alerts from well-known anti-virus software organizations. A particularly dangerous form of spam is "phishing", which is the attempt to acquire sensitive information (such as usernames, passwords, and credit card details), or for delivering harmful viruses and malware, by posing as a trustworthy entity in an email communication.

For the average business, sophisticated top of the line enterprise-grade spam solutions that proactively stay on top of changing tactics can be cost prohibitive. Many of the standard "off the shelf" filtering solutions are only updated monthly and will not block the latest evolving tactics until it's too late.

ANTI-SPAM/ANTI-PHISHING FILTERING BEST PRACTICES

The Rackspace spam filtering system is continually updated and employs 3 layers of scanning that eliminates 98% of all spam in our Hosted Exchange mailboxes—with nearly zero false positives (legitimate messages marked as spam).

Layer 1: The Gateway Scan – As soon as an email arrives, our gateway servers try to match the sending IP address to an aggregated blacklist compiled from multiple spammer tracking systems. The servers analyze the email message in comparison to other arriving mail. If a large number of emails arrive simultaneously from a single IP, or are addressed to users that do not exist in our system, it could signify a spam attack, and the servers block the offending email. Similarly, if the sending address is from a domain in our system but the mailbox does not exist, the servers block the email.

Layer 2: Cloudmark® Scan – We scan all email with Cloudmark's industry-leading spam detection software. Cloudmark uses Advanced Message Fingerprinting™ to detect spam and phishing. Advanced Message Fingerprinting uses algorithms that detect spam across all languages and character formats. These algorithms update every 60 seconds based on worldwide feedback loops and the latest spam tactics.

Layer 3: The Message Sniffer Scan – We scan email with Message Sniffer from ARM Research Labs. Message Sniffer relies on pattern recognition and machine learning technology to detect spam and phishing. It searches the entire message for spam, including unusual headers, message source behaviors, structural artifacts, obfuscation techniques, binary and image signatures, email and URL targets, unusual code fragments, and even coding styles.

The Rackspace Dedicated Exchange product offers customers Symantec Spam and Virus protection; an industry leader in spam intelligence and proactively protecting data.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Does your current anti-spam solution still result in spam emails getting through on a daily basis?
2. Do you get a number of legitimate emails sent to spam folders?
3. Are you concerned that you are still at significant risk for viruses and malware attacks?

#3 Anti-Virus/Anti-Malware

There are literally millions of computer viruses worldwide, and many of them are distributed via email. Current research by leading security organizations indicates 2-4% of all emails contain a virus.[4] That represents over 6 million email viruses being sent out every day. Like spam, the nature of the viruses is ever-evolving in an attempt to evade anti-virus software. Many standard "off the shelf" anti-virus solutions do not have the sophistication or capabilities to stay on top of the daily evolution of viruses and malware as updates are not conducted on a daily basis.

ANTI-VIRUS/ANTI-MALWARE BEST PRACTICES

Rackspace utilizes a set of highly sophisticated enterprise-grade solutions to guard against threats. Our systems block more than 100,000 virus-infected emails every day. During new virus outbreaks, our systems can block over 1 million messages per day. Rackspace Hosted Exchange includes multi-stage, server-level virus detection. Our virus scanning system can handle spikes for long periods of time, processing email without causing delays. We employ a 4-stage process:

Stage 1: Restricted Attachments – First we scan messages for dangerous types of file attachments. Dangerous files can execute code, which can be used by hackers to spread viruses or damage your computer. Restricted file types include, but are not limited to, program files (.exe, .com), script files (.bas, .vbs, .js), and shortcuts to files (.lnk, .pif). When an email containing a restricted file attachment is detected, the system rejects the email and the sender receives a "bounced" email notification.

Stage 2: Normalization – This stage of the email anti-virus process searches for formatting vulnerabilities that can hide viruses from scanners. If the system finds any vulnerability, it corrects the formatting of the message so that it can be thoroughly scanned (this is called "normalizing" the message). Normalization helps protect against known Microsoft Outlook® security threats.

Stage 3: Decompression – Many of today's viruses use compression as a way to sneak past virus scanners, sometimes even compressing themselves several layers deep. If the email contains any compressed attachments such as .zip files, the system temporarily unzips them and scans for viruses. If an attachment (such as a password-protected .zip file) cannot be decompressed, our system scans the original file for virus signatures that occur within compressed attachments.

Stage 4: Virus Scan – After the first 3 steps are complete, an email anti-virus scanner processes the email and the uncompressed attachments. This helps to provide maximum protection against new virus threats. Our system automatically updates virus definitions hourly, giving customers protection from new viruses within minutes (versus once per day for most anti-virus solutions).

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Are you aware of the full capabilities of your current anti-virus solution? How does it compare to the above 4 stage process?
2. Are your network, servers, and/or individual employee computers regularly found to have viruses and malware?
3. Do you spend precious time and resources dealing with viruses and malware versus focusing on more important IT initiatives?
4. Are you concerned with diminished employee productivity due to virus/malware attacks?

#4 Managing Security Patches and Updates

Keeping Exchange Server and its supporting infrastructure up to date with security patches, OS patches, hotfixes, hardware updates, and service pack updates is a time consuming process, let alone the monthly server maintenance that should also be conducted. Many IT staff hours are spent running the updates, and at times, fixing configuration issues caused by the updating process. While just a rough estimate, it isn't unrealistic to spend 10 or more hours per month per server on patches and maintenance-related activities.

With IT resources spread thin and only so many hours in the day, time spent on managing Exchange Servers and infrastructure takes away from other important initiatives. As a result, either the patching and update process doesn't always get done in a timely manner (within a couple of days), or if it does, other projects will suffer. Furthermore, some patches are for fixing critical security issues that leave you potentially vulnerable if they aren't immediately addressed.

MANAGING SECURITY PATCHES AND UPDATES BEST PRACTICES

Rackspace employs hundreds of professionals whose sole focus is to manage Microsoft Exchange environments. All Hosted Exchange environments remain up to date with all Exchange Server and Windows Server security patches and updates.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Are security patches and updates currently deployed within a few days?
2. How many hours per month does your IT staff spend managing your infrastructure, and is that time at the expense of more strategic IT projects?
3. Is your IT staff up to date on the most current Exchange Server and Windows Server training and certifications?

A Special Note for Users of Exchange Server 2003

For organizations still running Exchange Server 2003, you are in a special risk class. Exchange Server 2003 is now at ***END OF LIFE.***[5] *It is no longer supported by Microsoft. There are no additional security patches, updates, or phone and/or email-based support from Microsoft. Continued use can make you especially vulnerable to newly developed security threats.*

C. Downtime Issues

Security is obviously very important, but so is downtime. Given the fact that email is a mission-critical application, minimizing downtime should be a high priority for all organizations. There are a number of factors that contribute to Exchange Server downtime or add to the risk of unplanned downtime occurring, including:

- Older hardware and infrastructure
- No redundancy in place
- Lack of a robust disaster recovery plan and process in place

A recent study by Osterman Research[6] found that the typical email system experiences a mean **unplanned** downtime of 43 minutes during a typical month, or eight hours and 36 minutes per year. Moreover, the typical system is down for a mean of 85 minutes per month for **planned** maintenance, or 17 hours per year. Based on a 24x7 operation, the total unplanned and planned downtime of 25 hours 36 minutes per year equates to an uptime of 99.7% for on-premises systems.

Further, Osterman Research estimates that the average email user is about 25% less productive during periods of email downtime.[6] Assuming that the fully burdened, average labor rate for the typical email user is $35 per hour, a one hour email outage every two months for 1,000 users will cost $52,500 in lost productivity each year.

Thus, minimizing unplanned downtime should be an important strategic initiative for IT as even 99% availability represents over 87 hours per year of unplanned downtime.

MINIMIZING DOWNTIME BEST PRACTICES

Based on Rackspace redundant architecture and global data center footprint, we are able to deliver a 100% Network Uptime financially-backed guarantee.

This means that we guarantee that our data center network will be available 100% of the time in a given month, excluding scheduled maintenance, which includes Rackspace managed switches, routers, and cabling. Based on our SLA, we will credit your account for each 30 minutes of network downtime for the affected server.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. What is your current in-house (or email provider's) availability? Does it exceed 99.99%?
2. What is your total cost per one hour of email downtime?
3. What is your recovery plan in the event of unplanned downtime?

#5 Hardware and Infrastructure

The older your servers, networking equipment, applications, and operating system are, the greater the risk of failure.

Hard drives are the most likely point of failure in older hardware since they have moving parts. A hard drive failure usually results in severe data loss, and data recovery attempts may cause further damage if not executed correctly.

There is also the issue of "bit rot", this is the idea that bit in memory or on a disk can silently decay. As disk capacities, file sizes, and the amount of data stored on a disk increases, the likelihood of the occurrence of bit rot and other forms of uncorrected and undetected data corruption also increases. While the error rate of enterprise-grade hardware may seem incredibly low, as you increase the amount of stored data, your chances of being impacted can go from trivially low to a rate that can be concerning.

Older versions of Exchange Server can also suffer from "software rot". Software rot describes the process of a slow deterioration of software performance over time or its diminishing responsiveness that eventually leads to it becoming faulty, unusable, and/or otherwise categorized as "legacy" and in need of upgrade.

HARDWARE AND INFRASTRUCTURE BEST PRACTICES

To guard against failure, Rackspace employs and maintains enterprise-grade servers and networking equipment for both our multi-tenant cloud platform and customized dedicated offerings. We also provide a one-hour hardware replacement with a financially-backed guarantee for customized Exchange deployments (for both Managed™ and Intensive® service levels). Rackspace completely manages and maintains the servers to help ensure all hardware components are functioning, and replaces any failed components at no cost to the customer.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Are you relying on servers and networking equipment older than 7 years?
2. Is your capital expenditure budget hindering your ability to update your hardware and infrastructure?

#6 Redundancy

The best way to avoid unplanned downtime is to remove single points of failure through redundancy. This should include everything from your server and networking infrastructure to your specific Exchange Server(s). It can be expensive to implement full redundancy and as a result, many companies lack a level of redundancy to guard against downtime.

REDUNDANCY BEST PRACTICES

Rackspace global data centers can provide geographic redundancy and deliver a 100% network uptime guarantee along with industry leading SLAs. This is made possible based on our industry-leading data center architecture, which includes:

Network

- High-performance bandwidth
- 9 network providers, for multiple redundancies
- Over 200 CDN edge locations on 6 continents optimize content delivery: North America; Europe; Asia-Pacific; Africa; South America; Middle East
- Fiber carriers that enter at disparate points to guard against failure
- Network topology and configuration automatically improves in real time
- Configuration, co-developed with Cisco, guards against single points of failure at the shared network level (extendable to your VLAN environment)

Core routing equipment

- Fully redundant, enterprise-class routing equipment
- Fiber carriers enter at disparate points to guard against service failure

Rackspace can also architect a customized Exchange environment to meet your specific availability and redundancy requirements.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Is your on-premise infrastructure resilient in the event of an unplanned event?
2. Do you have automatic failover in place to ensure maximum uptime?

#7 Backups and Disaster Recovery

When you hear the word "disaster" you tend to think of extreme events such as earthquakes, hurricanes, tornados, floods, or fire. But in reality, these are low probability events. The most common causes of unplanned downtime include[7]:

- Human error
- Hardware and software failure
- Cybercrime/hackers
- Malware/virus attack
- Power outage

It should be stated that backups and disaster recovery are two very different things. The backup process merely ensures that your data is protected, but it usually lacks a "recovery" process, and backups can sometimes fail, leaving you with less data protection than you thought.

Having a disaster recovery plan in place, and the ability to effectively implement that plan in the event of a disaster, ensures maximum availability of your Exchange email. There is a wide array of approaches to implementing a disaster recovery solution. Implementing the right solution on-premises should be based on: (1) your cost of downtime, (2) your recovery point objective (RPO) which is how much data you can afford to lose measured in minutes, hours, days, or weeks, and (3) your recovery time objective (RTO), or how quickly you need to be back up and running after a disaster (measured in minutes, hours, days, or weeks).

Most on-premises Exchange configurations employ a simple daily backup of all mailboxes. This assumes your organization is comfortable with losing up to 24 hours worth of data. Getting the back-up files up and running again may take up to a few days (depending on resources and back-up location).

Backups and Disaster Recovery Best Practices

Rackspace Hosted Exchange provides a 100% network uptime guarantee. Our Hosted Exchange solution takes daily mailbox snapshots which enables end-users to recover messages in Outlook for up to 14 days, or can restore an entire deleted mailbox for up to 30 days. Rackspace also provides an email archiving service for an additional fee that provides unlimited email storage, retention, and recovery.

A dedicated Exchange environment provides an opportunity for a more customized approach to data retrieval, redundancy, and disaster recovery. Your environment can be architected to meet your exact business requirements, including multiple copies in geographically dispersed data centers, archiving, and customized RPOs and RTOs.

HOW DO YOU COMPARE? KEY QUESTIONS TO CONSIDER

1. Do you have a backup and/or disaster recovery plan in place?
2. How much would one hour of Exchange server downtime cost your organization?
3. How long would it take to get back up and running after an event?
4. Are you confident that your backups actually work?

D. Conclusion

We've provided a high level comparison of some of the key security and downtime challenges organizations need to address with their on-premises Exchange email system. We've also reviewed the approach Rackspace delivers to help you better compare the two so you can determine the right approach for your organization. Rackspace successfully delivers over a hundred million emails every day on behalf of our customers. Most of our customers were either running their own Exchange servers on-premises, or were using a free email service from a hosting provider. Our customers weighed the costs and the benefits or their current approach and concluded it made more sense to move to Rackspace. For more information on Rackspace email solutions, visit us at http://www.rackspace.com/email-hosting/.

Appendix

Rackspace Exchange Email Solutions

Solution	Hosted Microsoft Exchange at Rackspace	Dedicated Microsoft Exchange at Rackspace	Microsoft Exchange Hybrid at Rackspace
Description	A multi-tenant (shared) version of Microsoft Exchange, purchased per mailbox and delivered from Rackspace data centers.	Customized Microsoft Exchange Server delivered on dedicated hardware specific to the customer. Rackspace can architect the environment to meet particular business requirements.	Microsoft Exchange Hybrid is the best way to handle email users with different needs, while saving money. Power users get the robust features of Hosted Microsoft Exchange, while casual users enjoy affordable, POP/IMAP Rackspace Email – all on the same domain.
Ideal Use Cases	• Meets the needs of most organizations requiring an enterprise-grade email solution • Best solution if you desire a per user, per month pricing model • No Exchange expertise needed • No customization needed	• Customized feature set and/or dedicated hardware requirements • Security or compliance requirements that call for a single tenant solution • Customized backup or disaster recovery configurations • Integration with other custom business applications	A cost savings measure when you have a mix of users requiring the full feature set of Hosted Exchange, as well as a group that only requires a basic business email solution
Detailed Product Information	http://www.rackspace.com/email-hosting/hosted-exchange/	http://www.rackspace.com/managed_hosting/services/dedicated_exchange/	http://www.rackspace.com/email-hosting/webmail-exchange-hybrid/

References:

1. Osterman Research, "Results of a Survey with Email Users", April 2013 http://www.ostermanresearch.com/freeresearch/rsch_0180.pdf
2. InformationWeek 2014 Strategic Security Survey, http://reports.informationweek.com/abstract/21/12509/Security/Research:-2014-Strategic-Security-Survey.html
3. Dimensional Research, "The State of Corporate Email", October 2013 http://www.dimensionalresearch.com
4. Kaspersky Labs, "Spam and Phishing Statistics Report Q1-2014" http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.VHYypMt0zcs
5. Microsoft Product Lifecycle, http://support2.microsoft.com/lifecycle/search/?alpha=Exchange+Server&wa=wsignin1.0
6. Osterman Research, "The Case for Hosted Exchange", December 2012 http://www.rackspace.com/knowledge_center/whitepaper/the-case-for-hosted-exchange
7. The Disaster Recovery Preparedness Council, "The State of Global Disaster Recovery Preparedness," 2014 Annual Report, www.drbenchmark.org.

About Rackspace

Rackspace® (NYSE: RAX) is the #1 managed cloud company. Its technical expertise and **Fanatical Support®** allow companies to tap the power of the cloud without the pain of hiring experts in dozens of complex technologies. Rackspace is also the leader in hybrid cloud, giving each customer the best fit for its unique needs — whether on single- or multi-tenant servers, or a combination of those platforms. Rackspace is the founder of OpenStack®, the open-source operating system for the cloud. Based in San Antonio, Rackspace serves more than 300,000 business customers from data centers on four continents.

GLOBAL OFFICES

Headquarters Rackspace, Inc.
1 Fanatical Place | Windcrest, Texas 78218 | 1-800-961-2888 | Intl: +1 210 312 4700
www.**rackspace**.com

UK Office
Rackspace Ltd.
5 Millington Road
Hyde Park Hayes
Middlesex, UB3 4AZ
Phone: 0800-988-0100
Intl: +44 (0)20 8734 2600
www.rackspace.co.uk

Benelux Office
Rackspace Benelux B.V.
Teleportboulevard 110
1043 EJ Amsterdam
Phone: 00800 8899 00 33
Intl: +31 (0)20 753 32 01
www.rackspace.nl

Hong Kong Office
9/F, Cambridge House, Taikoo Place
979 King's Road,
Quarry Bay, Hong Kong
Sales: +852 3752 6488
Support +852 3752 6464
www.rackspace.com.hk

Australia Office
Rackspace Hosting Australia PTY LTD
Level 1
37 Pitt Street
Sydney, NSW 2000
Australia

Modified: 062015