Overcoming Exchange Failures: Beyond Traditional Backups

Addressing the Need for Both Speed and Granularity of Recovery

More and more, organizations of all sizes are harnessing the power of Microsoft Exchange Server and Outlook to support business processes closely tied to revenue generation and high levels of customer support. Availability of e-mail and associated data can impact an organization's ability to make or break a quarter – as well as retain or lose customers. In today's economy, the importance of e-mail takes on new meaning. Recovery time and recovery point objectives (RTOs and RPOs) are no longer general rules. The Exchange administrator's ability to meet or exceed the proverbial lines in the sand, in terms of time to recover and the age of the data recovered, can mean the difference between gainful employment and prepping for a job interview. This paper takes a close look at the impact of e-mail downtime on today's business, the types of failures – both the common and the not-so-common along with the general probability of occurrence and the typical impact. Also spelled out are some ways to mitigate the impact of these challenges to ensure adequate levels of protection for your Exchange environment.

Business Dealings in the 21st Century

Anyone who witnessed the growing corporate reliance on e-mail should not be surprised at the impact e-mail now has on day-to-day operations. An individual's ability to send and receive e-mails, predominantly via Microsoft Exchange, now tends to outweigh more traditional modes of business communication.

As much as 97 percent of all business communications now occurs via e-mail. [1]

- Important client and partner relationships are developed, cemented and nurtured based on the ongoing e-mail conversations and agreements between parties.
- Details of important contracts and business negotiations are often ironed out in e-mail form.
- Business strategies are plotted and revised, purchase orders are communicated and services rendered via e-mail.
- Cross-departmental communication between different members of a company's functional teams also occurs regularly via e-mail.

The Impact of Downtime

Despite its prevalence in the market, the true business impact of e-mail is often felt only by its absence. Losing minutes or hours of e-mail connection quickly adds up and can greatly affect productivity.

Self-proclaimed Tech of All Trades Tim Malone summed up the very real human impact of e-mail failure in a blog posting that chronicled an e-mail outage at his company:

> *"I don't know how critical e-mail delivery is in your organization but in our business, it is the life-line of just about everything we do. So much depends on our e-mail system functioning properly. We could function without our accounting system for a day but it is possible that somebody could lose their job if the e-mail system were to be out for more than a few hours. People tend to get real nasty when they can't get e-mail."* [2]

In the wake of an Exchange outage, the erosion of a company's bottom-line profits and productivity can be significant. As shown in Table 1, any critical system downtime can cause substantial financial impact to the average 500-person corporation.

IN THE WAKE OF AN EXCHANGE OUTAGE, THE EROSION OF A COMPANY'S BOTTOM LINE PROFITS AND PRODUCTIVITY CAN BE SIGNIFICANT.

Table 1. Average Yearly Cost of Downtime for a 500-Person Corporation

Type of Disruption	Downtime Events Per Year	Avg Hours of Downtime Per Event	Avg Total Downtime	Industry Avg Cost
Server Crash	2	26	52	$ 936,000 [3]
Data Corruption	4	4	16	$ 288,000
Storage Offline	4	4	16	$ 288,000
Total			84	$ 1,512,000

What Do We Know About E-mail Outages and Their Impact?

As you look more closely at the average operation of e-mail systems in companies, the impact of even a single outage becomes more significant. Table 2 summarizes findings from various e-mail operations surveys, including

- The cost impact of e-mail downtime
- The likelihood of an e-mail outage occurring
- The average duration of an e-mail outage
- How many companies can keep sending and receiving e-mail after a failure

Table 2. Specific Impact of E-mail Downtime

Estimated Cost of E-mail Downtime	
Overall Annual Cost	Up to $500,000 [4]
Annual IT Support Cost	$36,800 [5]
Chance of E-mail Downtime Over a 12-Month Period	
Chance of Unplanned Downtime	75% [6]
Chance of Planned Downtime	14% [7]
Duration of the Average E-mail System Outage	
Average E-mail System Downtime in a Given Month	69 minutes [8]
Average E-mail System Downtime Over 12 months	32.1 hours [9]
Ability to Keep Using E-mail After a Server Failure Occurs	
Percent of Businesses Able to Send and Receive E-mail Without Interruption or Data Loss After Server Failure	36% [10]

ORGANIZATIONS TEND TO EXPERIENCE AN AVERAGE E-MAIL SYSTEM DOWNTIME OF ROUGHLY 32 HOURS IN ANY 12-MONTH PERIOD.

When it comes to restoring e-mail from some type of local, planned or unplanned outage, it's not so much a question of what you can do if you ever need to restore e-mail. The better question is: What can you do the next time e-mail operations are interrupted?

IT professionals must take time to evaluate whether or not their current Exchange data protection technologies and processes are indeed sufficient to meet the needs of their organization both in terms of recovery time and recovery granularity. These evaluations should be done on a regular basis and take into consideration not only the increase in Exchange data being stored, but the importance of e-mail to the health of the organization in terms of revenue generation, customer service and compliance. As the criticality of e-mail increases, recovery point and recovery time objectives will undoubtedly be reassessed. IT will often have to go back to the drawing board to plan accordingly.

Simplified Protection of Exchange When Using Traditional Backup Policies

For some organizations, traditional backup policies – a combination of weekly full, differential and transaction log backups – is the preferred method of data protection for Exchange. Whether coupled with tape or disk, traditional backup and recovery has long proven reliable and for some organizations may remain the preferred approach.

One thing to keep in mind when considering traditional backup policies is that some gaps in protection are unavoidable. There will be periods of time between backup jobs where Exchange data is left unprotected and in turn is more susceptible to loss in the event of a failure. The amount of data loss is solely dependent upon the defined backup routine. Whether or not this a serious concern falls back on the individual organization as the perceived value of Exchange data varies considerably One other thing to point out when considering traditional backup policies is that the recovery of data is often a slow, labor intensive process. In some cases multiple attempts are required to ensure the data recovered is actually useable. That being said, for organizations that can easily bounce back from as much as 12 hours of lost Exchange data, as well as extended periods of downtime during the recovery process in which e-mail will be unavailable, traditional backup policies may be good enough. Even then, there are ways of improving and simplifying the task.

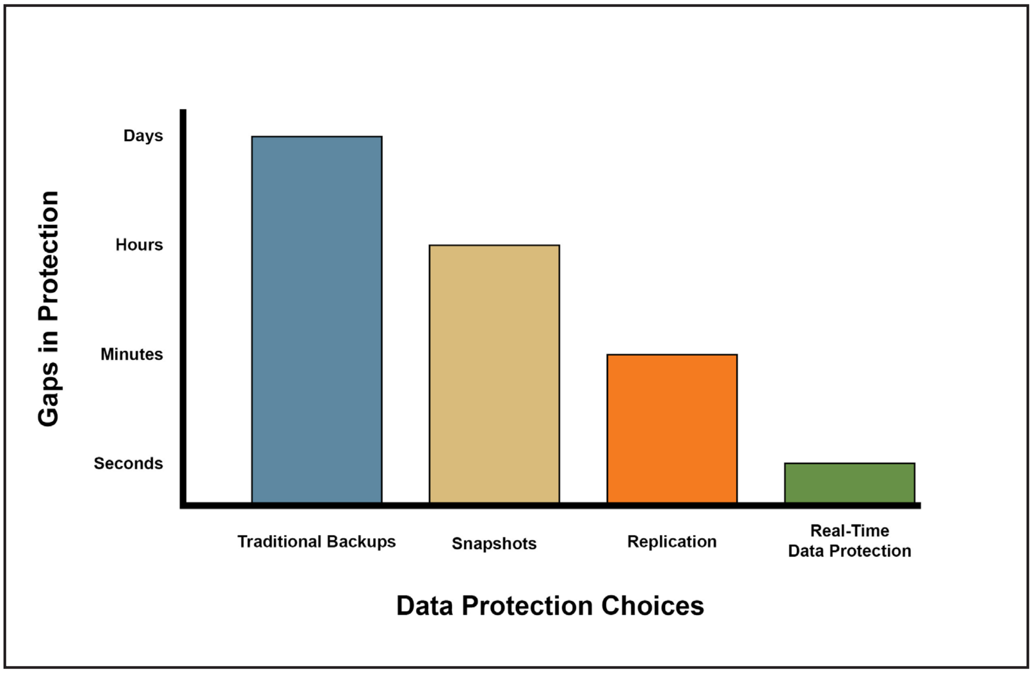
Restoring complete information stores, individual storage groups or individual databases should not require the expertise of an Exchange database administrator (DBA). For users, this equates to faster recovery and improved productivity.

When Time is of The Essence - What to Do When Exchange Recovery Needs to Happen Now

Many companies continue to practice traditional data protection methods for their Microsoft Exchange environments. This may take one of many forms, including

- Weekly full backups with nightly, differential backups to tape
- Scheduled snapshots
- Continuous replication (mirroring) to a local or remote disk-based storage system

HOW QUICKLY WILL YOUR SOLUTION LET USERS START SENDING AND RECEIVING E-MAIL AFTER AN OUTAGE?



While each of these methods offers strengths in data protection and disaster recovery, organizations must consider and fully understand the impact of Exchange downtime and data loss on the viability of their business. What bad things will happen as a result of an e-mail outage? How might “minor issues” snowball into career threatening outages? In terms of recovery point and recovery time objectives, what are users expecting? What about regulatory/compliance demands? Each of these considerations should be factored into defined recovery point and recovery time objectives for Exchange.

Table four details some of the typical challenges facing data administrators during an Exchange Server outage. These challenges are compared against key factors affecting Exchange protection, such as the different levels of data protection and frequency of backups.

Table 4

Type of Failure (Challenge)	Probability Of Occurrence	Typical Impact	Continuous Protection	Traditional Backup Policies	Bare Metal Recovery	Monitoring
Over-running the defined backup window	High	Moderate to Very High	X			Preventative Measure Only
Loss of Individual E-mail	High	Moderate	X			Preventative Measure Only
Loss of Mailbox	High	Moderate to very high	X			Preventative Measure Only
Isolated Database Corruption including Virus Corruption	High	High	X	X		Preventative Measure Only
Complete Database Corruption including Virus Corruption	Medium	Very High	X	X		Preventative Measure Only
Isolated Media Failure	Medium	High	X	X		Preventative Measure Only
Complete Media Failure	Low	High	X	X		Preventative Measure Only
Loss of Entire Exchange Server	Low	Very High			X	Preventative Measure Only
Loss of Entire DataCenter	Low	Extreme			X	Preventative Measure Only

Challenge: Over-running the defined backup window

As the power and convenience of e-mail works its way into critical business processes, the amount of data associated with this powerful tool continues to spin out of control. This poses challenges for organizations of all sizes in terms of completing backup jobs within the defined window – outside of normal business hours. At the end of the day, Over-running backup windows can impact an organization in several ways.

A notable degradation in Exchange Server performance is common during backups. This is why backup administrators make it a point to schedule backup jobs during the wee hours of the morning and on weekends – times where email traffic is minimal. Users don't take kindly to sluggish e-mail performance – especially when it becomes a speed bump in the path of booking revenue during a quarter end push, or as a customer's patience grows thin during a critical support issue.

Over-running Exchange Server backup windows also leads to periods of time where data is left unprotected because of the inability to start the next backup job while the previous one has not yet completed. How much Exchange data can your organization afford to leave unprotected for any period of time? This is a question that must be asked and answered when formulating a data protection strategy.

Question to Ask Your Backup and Recovery Vendor:

How can I avoid gaps in data protection, as well as contend with data growth while ensuring that my backups are always completed within the designated window?

Challenge: Isolated or complete Exchange database corruption, including virus corruption, and isolated or complete media failure

Sometimes patches, viruses or other elements introduced into the Exchange environment can lead to data corruption that may ultimately bring down your Exchange system. Even though your organization may perform regular backups or local or remote replication, chances are high that your most recent backup data may also be corrupted.

This can create a few issues when it comes to recovery:

- If your last data set has been corrupted, recovery can require significant administrative time, extra passes and many application checks before the data is perceived as usable by Exchange. In the meantime, your users are left idle as they wait for Exchange to become available.
- If you decide to go farther back in time and restore an earlier data set from a known good state, your environment may then be subject to a large amount of data loss.

Question to Ask Your Backup and Recovery Vendor:
How does your solution protect me from potential data corruption?

Challenge: Loss of individual e-mail or an entire mailbox

Many Exchange administrators plan their data protection schemes around just the ability to perform a full restore of their Exchange Server. However, it's much more likely for the backup administrator to receive a request for a specific e-mail message or the contents of an individual user mailbox to be restored. This can pose issues, such as

- **How quickly the lost item can be located.** A manual restore process may require the administrator to search for and analyze individual mailboxes to locate the correct item(s) to be restored. Trying to locate these items through backup tapes, staging the backup, and navigating Microsoft Recovery Storage Groups can complicate efforts and require extra recovery time. Suddenly the simple task of recovering the lost item may take an entire afternoon.
- **Extra backups and backup storage may be required.** Some data protection solutions offer a secondary backup process, known as brick-level backups, which allow administrators to more easily restore just the individual mailboxes or e-mail messages. This is a viable solution; however it still may not go far enough. Adding brick-level backups on top of other Exchange backup processes can strain backup and network resources, dramatically impact the backup window and tend to require a whole lot more storage. They also risk potential data loss between backups.

Question to Ask Your Backup and Recovery Vendor:
What extra steps do I need to take in order to restore individual mailbox items or specific user mailboxes?

Challenge: Loss of entire Exchange Server or entire datacenter

Many traditional backup and recovery solutions rely on tape as a tested, reliable, cost-effective means for storing data offsite. However, the downside of tape is that after a failure, a multi-hour recovery process may be required. During the recovery period, users are not able to send or receive e-mails, view or create new calendar entries, update tasks or access contact information. If the availability of e-mail is truly critical to the continued success of your organization, you must plan accordingly for the less likely, but very high impact failures such as the loss of an entire Exchange Server or even more unfortunate, the loss of an entire datacenter.

Questions to Ask Your Backup and Recovery Vendor:
How quickly does your solution let users resume sending and receiving e-mail after an Exchange outage occurs? If necessary, can I recover data to an alternate physical server or a virtual machine?

Meeting Exchange Data Protection Challenges

There is one solution today that combines disk-based, real-time backup and any point in time, extremely fast recovery for Exchange – as well as SQL Server and Windows File Servers – NetVault: FASTRecover. It eliminates one of the biggest data protection challenges for organizations of all sizes – backup windows. Thus removing the concern of backups overrunning their scheduled windows, affecting productivity and stranding the most current data, unprotected. Always on - capturing and backing-up byte-level changes to protected data sets as they occur, there is no longer a need for recurring traditional full and incremental backups beyond off-site, archival requirements.

NetVault: FASTRecover's Virtual On-Demand Recovery™ technology makes these critical applications and associated data available for use in as little as 30 seconds, meeting even the strictest recovery time objectives. Plus, recovered data is completely useable by the application on the first recovery – eliminating wasted time and multiple recovery attempts. NetVault: FASTRecover also allows for granular "rewind." In the event of data loss or corruption, you can roll back to any-point-in-time, down to the second, to retrieve valid data.

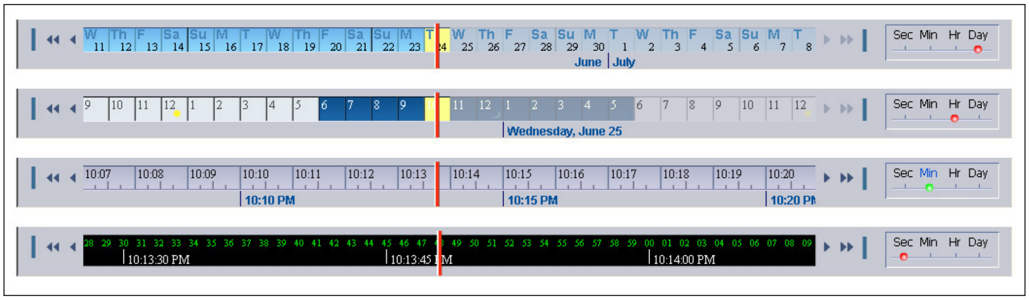


Figure 1. NetVault: FASTRecover's granular "Rewind" by Day, Hour, Minute, or Second

Available as a software-only solution, or as a pre-configured appliance, the user can leverage existing resources with the software or source the appliance to simplify installation. Integration into a user's existing environment is also hassle-free. NetVault: FASTRecover is compatible with traditional backup applications, allowing the recovery data stored in NetVault: FASTRecover's Online Storage to be archived to tape and stored offsite. NetVault: FASTRecover fits seamlessly into existing backup infrastrucutres, a rip and replace of existing backup applications is not required.

For users looking for additional data protection solutions, it is recommended that the following applications be considered for Exchange data.

NetVault: Backup APM for Exchange Server increases confidence in the recoverability of Exchange. Support for online backups via Exchange Server's Extensible Storage Engine (ESE) and Volume Shadow Copy Service (VSS) provides users the flexibility to select their preferred backup method to create flexible backup policies that account for multiple recovery scenarios without learning Exchange internals.

NetVault: Bare Metal Recovery can reduce the task of rebuilding a disk to a matter of hours. When combined with NetVault: FASTRecover and NetVault: Backup and the Exchange Server APM, NetVault: Bare Metal Recovery provides an added level of protection in the fight to ensure business continuity.

NetVault: Report Manager Pro for Exchange (NRME) integrates Exchange storage and management reporting so administrators can efficiently analyze and manage storage. Reports yield actionable information that enables storage forecasting, reduces storage growth rates, lowers administrative costs, increases security and enhances regulatory compliance.

BakBone's Exchange Data Protection Solutions

NetVault: FASTRecover
- Elimination of backup windows
- Lightning fast recovery of data
- Simple plug-and-play deployments to fit your budget
- Works with your existing backup application
- Restore Individual Mail Items Directly to Same or Alternate Mailbox

NetVault: Backup and Exchange Server APM
- Full, incremental and differential backups
- Copy-only backup
- Protection down to the individual database level
- Point-and-click UI

NetVault: Bare Metal Recovery
- Simplifies and expedites the process of bare metal recovery
- Automates recovery of operating systems, network settings, system settings, applications, disk partitions and data

NetVault: Report Manager Pro for Exchange
- Creates detailed analysis of users' e-mail disk space consumption and e-mail traffic flow
- Increases storage utilization in Exchange environments
- Reduces exchange storage growth rates
- Maximizes Exchange administration

Conclusion

Many of today's corporate environments cannot tolerate the repercussions of a future Exchange outage. Getting e-mail up and the company back to business is essential to maximizing productivity and enhancing customer relations, and at the end of the day, is essential to your company's bottom line. BakBone offers a wide range of Exchange protection and recovery options that are simple to use, improve recoverability and are a must for any organization that cannot be without Exchange or e-mail data for any length of time, even minutes or seconds.

References

1. “Preparing for email outages is a weak area in business continuity planning,” Aug. 29, 2008, Continuity Central, http://www.continuitycentral.com/news04116.html.
2. “When the e-mail system fails,” *Tech of All Trades* blog posting, Tech Republic, April 2, 2008, http://blogs.techrepublic.com.com/techofalltrades/?p=137.
3. *Annual downtime cost derived by multiplying the total hours of downtime per year by $18,000 per hour (average hourly cost of downtime, according to industry sources)*. Sources for downtime impact and cost data derived from the Contingency Planning Association and Strategic Research.
4. 47% of survey respondents estimated the cost of e-mail outage at either “up to $100,000” (27% of respondents) or “up to $500,000” (20% of respondents). Source: “Staff considerably upset by email downtime,” IT week, August 13, 2007, http://www.computing.co.uk/itweek/analysis/2196590/staff-considerably-upset-email.
5. Annual IT support cost for e-mail downtime is calculated per lost e-mail or file service ticket for organizations that handle 100 tickets per year, and spend an average of four hours of IT time per ticket (for a total time of 400 hours of IT support per year). Source for IT support costs and calculations: Contingency Planning Association and Strategic Research.
6. “Understanding Technical and Other Causes of Email Outages,” Disaster Resource.com, http://www.disaster-resource.com/articles/05p_102.shtml.
7. Ibid.
8. While the average monthly downtime surveyed was 69 minutes, many respondents clocked as much as 180-300 minutes of downtime. Source: “Staff considerably upset by email downtime,” IT week, August 13, 2007, http://www.computing.co.uk/itweek/analysis/2196590/staff-considerably-upset-email.
9. Even given the average outage duration of 32.1 hours, 43% of survey respondents reported e-mail outages of over 24 hours. Source: “Understanding Technical and Other Causes of Email Outages,” Disaster Resource.com, http://www.disaster-resource.com/articles/05p_102.shtml.
10. See Reference Note 1.

BakBone®
The Power of Simplicity™

BakBone Global Headquarters
9540 Towne Centre Drive, Suite 100
San Diego, CA 92121
Toll Free Phone: 877-939-2663
Phone: 858-450-9009
Fax: 858-450-9929
Email: sales@bakbone.com

Asia Pacific Headquarters
Shinjuku Dai-ichi-Seimei Bldg.11th Floor
2-7-1 Nishi Shinjuku, Shinjuku-ku
Tokyo, Japan 163-0711
Phone: 81-3-5908-3511
Fax: 81-3-5908-3512
Email: sales@bakbone.co.jp

Europe Headquarters
100 Longwater Avenue
Green Park
Reading
RG2 6GP
United Kingdom
Phone: 44 (0)1189-224-800
Fax: 44 (0)1189-224-899
Email: sales_europe@bakbone.com

85411_08-20-09