APPLICATION BRIEF
DISASTER RECOVERY AND ZANTAZ EAS

On August 28, 2005 the hurricane Katrina beat a path through the Gulf of Mexico directly toward New Orleans. Mandatory evacuations were ordered and hundreds of thousands of people fled the city leaving their homes and businesses behind. Less than 24 hours later, as winds hit 175 mph, Katrina made landfall on the Louisiana coast and the storm's rampage began. Two major flood-control levees were breached resulting in widespread flooding. At the Louisiana Superdome, where 10,000 people were taking refuge, huge sections of the roof were torn away by the gale. Across Louisiana, Mississippi and Alabama more than 1.3 million homes and businesses suffered what Mississippi Governor Haley Barbour described as "catastrophic damage."

With entire neighborhoods under 20 feet of water, New Orleans was left with no power, no drinking water, widespread looting and unchecked fires.

With entire neighborhoods under 20 feet of water, New Orleans was left with no power, no drinking water, widespread looting and unchecked fires. The entire region – 90,000 square miles, an area greater than the size of the United Kingdom – was declared a public health emergency. People were stranded in buildings, on roofs, or gathered on higher ground. The whole of the gulf coast was devastated and authorities feared the worst as disease spread through the contaminated, stagnant floodwater. The severity of this disaster is unprecedented and no one can predict ultimately how long recovery efforts will last.

The disastrous conditions left behind by Katrina remind us that preparation can be key to survival. And for businesses of all types and in all industries, a tried and tested contingency plan is essential in order to ensure that business operations can be recovered in the wake of a major disaster.

E-MAIL IS A CRITICAL BUSINESS COMPONENT

One critical component that is often overlooked in disaster recovery planning is e-mail. Electronic mail has become a cornerstone of corporate business and has quickly replaced written documents, faxes, and even the telephone as the primary communication conduit for most organizations. As computer technology has advanced and people have become accustomed to using e-mail, the importance and complexity of e-mail has evolved from a few simple text messages into a multitude of mission-critical documents. Negotiations, bids, proposals, contracts, legal agreements, regulatory forms, and a host of other vital correspondence now find form in electronic messaging systems.

One critical component that is often overlooked in disaster recovery plans is e-mail.

Indeed, e-mail has become so commonplace that it is hard to imagine getting along without it. Every day thousands of electronic messages are created as part of any company's operations. Americans send and receive well over 7 trillion e-mail messages each year, compared with only about 300 million pieces of first class mail. Studies show that the average office worker will dispatch and accept between 60 and 200 e-mail messages each day, and roughly two thirds of all American workers

use e-mail as part of their work routine. Nearly every key business process relies on e-mail as a critical component. As a result, suffering a system outage is a significantly damaging event for most, if not all, organizations.

E-MAIL RECOVERY

While many companies have various disaster recovery and business continuity plans, many also find that their programs fall short when it comes to e-mail. Messages are often widely dispersed in network servers and on individual hard drives throughout the enterprise. When backups are performed, e-mail data is often stored on tape drives or optical discs with out a cohesive management mechanism. Indeed, many organizations leave e-mail archive management in the hands of end users, making recovery in times of outage or disaster a hit-or-miss proposition.

Firms that overlook e-mail in their business continuity plans will find that recovering after a disaster may be a fatal impossibility.

This lack of focus on e-mail can spell disaster when it comes time to recover from a catastrophe. Firms that overlook e-mail in their business continuity plans will find that recovering after a disaster may be a fatal impossibility.

THE CHALLENGES E-MAIL ARCHIVAL

Clearly, the use of e-mail has grown dramatically in recent years; however, the size of e-mail (i.e., bytes) is increasing as well. In the early 1990's, most e-mail messages were between 1Kb and 3Kb in size, but basic electronic messages have grown over time, to a current average of 5Kb. In addition, a decade ago file attachments were rare, but today over 20 percent of e-mail comes with attachments. Graphic files, spreadsheets and Word documents are common. As a result, e-mail messages with attachments average around 100Kb today, and analysts predict that this super-sizing will continue at a growth rate of 35 percent per year.

The trouble with this exponential growth is that e-mail servers are designed to be transport vehicles, not archive repositories. Their ability to store data over time is limited, and as servers become overburdened by the volume system performance suffers. The result is slow response times, or worse, system outages when the servers themselves become unstable.

Analysts predict that the size and volume of e-mail will grow at a rate of 35% per year.

In an effort to manage unwieldy e-mailboxes, system administrators often use PST files as a "dumping ground" and automatically migrate e-mail from their users online message store to a PST file as messages age (i.e., older than "x months"). The trouble is that PST files are notoriously unstable; especially they grow in size, and this can foil attempts to recover critical information.

To combat the ever-growing demand on server storage and the inherent instability of PST files, system administrators often limit the allotted size of their users e-mail store. Today, the average size of a message store allotment is between 45 and 100 Mb. If a typical user sends and receives 70 messages per day (at an average of 5Kb) and 20 percent of

those messages have attachments (at an average of 100Kb), we can predict that users will quickly exceed their allotted storage space. As a result, most are forced either to begin deleting messages or find other places to store important e-mail.

Users often get around imposed limitations by storing e-mail in multiple places (often multiple times). Consequently, e-mail takes up residence in a hodge-podge of hard drives, laptops, and network servers of all sizes and types. Analysts indicate that overall space consumed by these unmanaged e-mails can be enormous – 10, 15, 20 terabytes, or more – and estimate that 30 percent of stored e-mail records and their attachments can be eliminated because they are redundant copies.

During disaster recovery, a centralized e-mail archive can be a lifesaver since mission-critical and historical e-mail is no longer spread out among various storage media, local hard drives and laptops.

CENTRALLY MANAGED E-MAIL ARCHIVE

Instead of allowing users to create ad-hoc e-mail archives or continuing to dump messages into unmanaged PST files, a better administrative approach is to create centrally managed archive designed to store large volumes of e-mail data and allow those messages to be retained and accessible at all times. This approach not only enables IT administrators to offload the burden on e-mail servers, improving their stability and performance, but it can ensure redundancy and access to critical messages in the event of a system outage or disaster.

During disaster recovery, a centralized e-mail archive can be a lifesaver since mission-critical and historical e-mail is no longer spread out among various storage media, local hard drives and laptops. Backup and recovery is achieved more quickly, completely and effectively with a centralized archive.

Establishing a centralized archive is only part of the equation, however. Organizations should be cautious to avoid a single point of failure. It is crucial that the central e-mail archive is included in overall corporate data recovery plans and redundant repositories should be established, preferably in separate geographic locations. To overlook this aspect of disaster planning will put the company at risk.

Establishing a centralized archive is only part of the equation, however. Organizations should be cautious to avoid a single point of failure.

As we see with the Katrina hurricane disaster – an event that impacted a three-state area – it does an organization no good to have an e-mail archive, only to have that archive suffer the same soggy fate at headquarters as other servers and systems. The risk is that during one singular problem – be it an electrical surge, a fire, or an event as catastrophic as a hurricane – the entire e-mail archive will be lost. The same type of business continuity acumen applied to phone networks, corporate data applications or network topology must be applied to e-mail archive management as well.

Another key aspect to making this redundancy work as an effective recovery mechanism is the ability to redirect operations between the redundant archives. If users typically access e-mail in New Orleans, for example, redirection to a redundant archive, say in Atlanta, is a must for recovery. Many companies on the gulf coast banked their recovery on data tapes or optical discs housed in their headquarters and are now suffering through a prolonged outage and recovery period. Some may not recover at all. Organizations with a broader recovery plan that

included backups in separate geographic locations have faired more favorably, incurring a relatively brief interruption of business operations.

AUTOMATIC ARCHIVAL AND REDUNDANCY VIA EAS

This redundancy and disaster recovery capability is intrinsic in ZANTAZ Enterprise Archive Solution (EAS). No additional replication tools or ancillary products are needed to ensure that e-mail is saved automatically in a centralized archive, and that the data in that repository is ported to one or more redundant storage sites. For example, as part of normal operation with EAS, e-mail system administrators can direct the archive to automatically replicate itself in multiple geographically diverse locations – New Orleans, Atlanta, Philadelphia, for example. These redundant repositories are updated on the fly by EAS as messages are archived.

The same type of business continuity acumen applied to phone networks, corporate data applications or network topology must be applied to e-mail archive management as well.

In the event of a disaster, message retrieval is automated as well. EAS will switch from its primary site to one or more redundant archives based on Microsoft IIS, the language of the majority of all Internet servers. If users request access to e-mail stored in New Orleans, but the server is down, EAS will automatically direct the request down another path to the secondary archive in Atlanta. If Atlanta is down also, EAS looks to Philadelphia, and so on.

This type of automated redundancy and re-routing is transparent to users, and part of the standard feature set of EAS. Administrators do not have to purchase ancillary products or manage additional tools in order to provide redundant protection and recovery capabilities. Users can work with the assurance that they can access important e-mail data via the centralized archive. Executives can rest a little easier knowing that the company has eliminated a critical point of failure that can put recovery out of reach during times disaster.

Firms must include redundant message repositories as part of their overall business continuity planning, a feature intrinsic to the basic functionality of EAS.

CONCLUSION

Unquestionably, e-mail has become a critical tool for efficient business communications. As a result, it is essential that organizations view the archive and retrieval of e-mail as a strategic imperative. Firms must include redundant message repositories as part of their overall business continuity planning. As we see with disasters like the Katrina hurricane and others, today's enterprises face huge challenges archiving and protecting the critical information housed in their e-mail stores. Zantaz EAS is an effective solution that is scalable, automated and secure. Using EAS organizations can take control and ensure that e-mail is protected and retrievable even during the worst catastrophic circumstances.