6 June 2008

Business Continuity Management

- ❖ Every year, 1 in 500 businesses will experience a severe disaster (London Chamber of Commerce)
- ❖ 43% of businesses that experience disasters never re-open and 29% close within 2 years. (McGladrey and Pullen)
- ❖ 90% of businesses that lose data from a disaster went bankrupt within two years of the disaster (London Chamber of Commerce)

Business Continuity Management (BCM) or a Business Continuity Plan (BCP), is a management process aimed at allowing an organisation to continue to function after (and ideally during) a "disaster", rather than simply being able to recover after a disaster.

This solution paper:

- ✓ Provides an overview of the BCM standards issued by APRA and ASIC, as their standards provide a detailed and practical "blueprint" for any organisation that is reviewing their disaster recovery preparedness.

- ✓ Examines in detail ZEB's offerings in the areas of: Data Backup, Data Recovery and Disaster Recovery that meet the requirements set out by APRA and ASIC.

APRA Guidance

In April 2005, APRA issued prudential standards on Business Continuity Management for authorised deposit-taking institutions and general insurers.[1]

BCM involves an integrated process of:

- Risk assessment;
- Business impact analysis;
- Consideration of recovery strategies;
- Business continuity planning;
- Establishing business continuity / crisis management teams and;
- Review and testing.

The standards provide practical direction in relation to *Risk Assessment*

- That the risk assessment should be undertaken at least annually and more frequently if there have been significant operational changes or new or changed external factors that would alter the business's continuity risk profile.

- That the worst case disruption scenario should be considered and include, but not be limited to:
  - o Loss of building;
  - o Denial of access to the building for a limited time;
  - o Loss of IT (data);
  - o Loss of IT (voice);
  - o Loss of vital (non-electronic records);
  - o Loss of key staff (temporary or permanent); and
  - o Loss of key dependencies (e.g. utilities, third party service providers and key suppliers)

[1]Prudential standards and guidance notes for authorised deposit-taking institutions: *APS 232 Business Continuity Management* and *Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management* and for general insurers: *GPS 222 Business Continuity Management* and *GGN 222.1 Risk Assessment and Business Continuity Management*

ASIC Guidance

ASIC has also set out requirements for Australian Financial Services (AFS) license holders; which broadly speaking, applies to all organisations that provide financial services.

Part 3 of the AFS Licensing Kit provides details on additional proofs required for the AFS License. The B5 Proof: Information Technology Capacity Statement (page 14), covers the processes for ensuring that the AFS Licensee has adequate information technology (IT) resources available to meet the AFS License holder obligations.

The B5 Proof requires the following areas to be addressed:

- your IT strategic plan;
- your IT disaster recovery plan; and
- your IT systems and systems functionality – you must demonstrate that your IT capacity is appropriate for your business (e.g. how often your electronic data is backed-up, whether you archive electronic files and / or store them offsite).

It will be clear to a reader of the APRA or ASIC guidance that business can face and need to have contingency plans in place for a number of different types of risk, and further that both bodies have determined that the probability of "Loss of IT" (APRA) or "technological and system risk" (ASIC) occurring to a business at some point is so likely that a risk-management plan is not only warranted – but required for this area of risk.

Hence authorised deposit-taking institutions, general insurers and businesses providing financial services are required (among other contingency plans) to have adequate Backup and Disaster Recovery Systems in place.

However the need for adequate data backup, data recovery and disaster recovery plans ought to be apparent to all managers; irrespective of whether the organisation falls within the scope of APRA / ASIC regulation or not.

The balance of this solution paper examines ZEB's offerings that address the:

- ✓ Data Backup;
- ✓ Data Recovery; and
- ✓ Disaster Recovery.

requirement of Business Continuity Management.

Data Backup and Recovery

The first line of defence in a disaster recovery solution is protecting the data. People often tend to think of their computer systems; the tangible equipment, as being valuable. What they often don't realise is that it's actually the data inside that has the greatest value. Computer equipment can be replaced the business data on the other hand is unique.

Our Online Backup System can scale from a single user system where all data is transferred automatically at a time determined by the user (up to 8 times per day if required for optimum "resilience"). In most cases clients keep copies of data to enable a recovery of up to 12 months before, but generally at least 3 months. This is known as a "backup window" and ensures that older copies of data (e.g. documents, e-mail, spreadsheets, accounts etc.) are recoverable.

All data transferred to one of our Backup Servers is encrypted using the AES algorithm. Once the pass-phrase has been entered by the user we are unable to view any of the data stored on one of our Backup Servers.

The base business backup package allows for up to 10GB capacity on our Backup Servers, with up to 1GB of compressed transfers per week. This system costs $10ex per week (billed 4 weekly in advance) with a setup cost (including software) of $250ex. This system also includes monitoring of the backup reports by ZEB and includes telephone support.

Organisations can use the same Online Backup System but use on-site disk storage as the primary repository for the backups (either Removable Hard Disks or a "Vault" (a NAS device), both of which can be deployed in an array for virtually unlimited storage capacity that provides the ability to increase storage capacity as needed).

Unlike the single user implementation, all backups are stored locally on the on-site disk storage and only a "mirror" of the most recent copy of the data on the server is automatically encrypted and synchronised off-site to one of our Backup Servers. This allows the Backup System to operate automatically and unattended, no tapes to change and no media to be rotated off-site.

The Backup System can also be configured to backup Microsoft Exchange mailboxes and other databases. If you would like to know more, click to read a case study about an Online Backup System which we have deployed for a 20 user site with Microsoft Exchange.

For details on the base Online Backup System with on-site disk storage using either 2 x 500GB RHD or an equivalent Vault click here.

The Online Backup System provides an affordable solution that addresses two of the questions posed by ASIC:

- ✓ Is your data regularly backed up?
- ✓ If the data is backed up, is your backup stored off-site?

System Backups

If the first line of defence in a disaster recovery solution is protecting the data, the second is undoubtedly protecting the application. By itself, the data provides a means for recovery – in time – however in reality the data doesn't exist in isolation.

For instance if you have a mail server, such as Microsoft Exchange, then if the Exchange application is not operational users will be unable to access the contents of their mailbox and further the organisation will be unable to send or receive e-mail. Similarly if an organisation's main line-of-business application utilises a database like Microsoft SQL Server, Oracle or SAP; then unless the actual database application is functional business operations will be severely disrupted as users will not be able to access the data contained within the database. Even 'simple' files such as documents and spreadsheets are normally stored on a network drive on a file server, if the file server is "down" then again the data is inaccessible.

In the preceding section we discussed Data Backups, which are typically performed at least daily. There is a second type of backup known as a System Backup, which unlike a Data backup copies the operating system, the registry and installed applications. Only a System Backup can restore a "broken" computer to an operational state, in the event that a computer will no longer start-up or one of the applications is no longer operational.

We can supply and install the necessary equipment to allow you to perform System Backups of your servers (or important workstations); the cost of this option using a 200GB USB backup drive is $780ex, for further details click here.

Data Recovery and Disaster Recovery

So far we have concentrated on backups: Data and System. We will now consider some scenarios where data loss has occurred and the options available to recover the data.

Scenario 1

User inadvertently deletes a whole directory structure that contains proposals sent to clients and other external correspondence.

The solution here is quite straight-forward and that is to restore the directory structure from the most recent backup. Provided data backups are performed nightly (the minimum recommended) the most work that would be lost would be the changes that had been made to files that day. However ZEB's Online Backup System can be configured to perform backups periodically throughout the day, and in that case, only changes made since the most recent backup earlier in the day would need to be re-entered.

Scenario 2

User inadvertently makes changes to a complex spreadsheet which invalidates the results; this error is not discovered for 3 weeks.

Again the resolution here relies on having a Data Backup System in place such as our Online Backup System, which is configured to provide a "backup window"; that is, a backup rotation scheme where multiple copies of data files are retained to allow prior versions of files to be restored when needed. We recommend that clients using our Online Backup System implement a 12 month Backup Window (i.e. have the ability to restore a version of a file up to 12 months old) and at a minimum implement a 3 month Backup Window.

Scenario 3

A patch for the database server corrupts the database rendering the database inaccessible.

Unlike the first two scenarios, in this instance as the database application is no longer operational; a restore from a System Backup would be required to return the server to a "pre-patch" state. This is a good example why it is good practice to perform System Backups prior to performing server updates as System Backups provide an excellent 'safety net' if application updates happen to go awry. If a System Backup had been performed prior to the patch being applied, a restore would typically take less than 2 hours to restore the server.

However if a System Backup was not performed prior to the patch being applied to the database server, then another option would be to contact the database vendor to seek assistance to troubleshoot and resolve the database error. With a reputable vendor, the troubleshooting approach is likely to succeed eventually, but it would likely take longer than 2 hours and might also require specialist assistance at additional expense, in a worst-case scenario it might be determined that the fastest resolution would be to re-install the database and restore the data from a backup (typically 1 – 2 days performed by a consultant).

Other options include a Standby Server or a failover solution which will examine further below.

Scenario 4

The RAID controller in the server experiences a hardware failure and corrupts the RAID array.

First we shall consider the recovery procedure if a Standby Server is not available. Because the RAID array is corrupt all data on the server has been lost, that means both a System restore and a Data restore will be required. However because the RAID controller has experienced a hardware failure, before the restore process can begin, the faulty RAID controller needs to be replaced. Let's assume that your supplier has a RAID controller in stock, allowing time for the initial fault diagnosis, obtaining and installing the RAID controller would likely take at least 4 hours and possibly the better part of a day. After that a System Restore is performed (say 2 hours), then apply any changes (e.g. add user accounts and mailboxes since the last System Backup), then perform a Data restore (say 2.5 hours). Then restore database backups and mailboxes since the last System Backup (say another 2.5 hours).

In short, you're looking at an outage of 1.5 to 2 days – and that's assuming that a replacement RAID controller is immediately available, if not the "down time" could be 3 days or even longer if problems are encountered.

This scenario provides a good example of two concepts associated with Disaster Recovery:

1. Recovery Point Objective (RPO)
2. Recovery Time Objective (RTO)

Most people are familiar with the concept of The Recovery Point Objective (RPO); which is to have the data restored and available for use.

However the Recovery Time Objective (RTO), the time taken to achieve the Recovery Point Objective; is often overlooked until a disaster occurs and the server is "down".

When the server is "down", operations are halted which costs money (and potentially reputation due to the inability to deliver core services).

There are a number of options which can reduce server "down time" in a disaster and provide committed Recovery Time Objectives. It then becomes a case of performing a cost of Disaster Recovery Option versus cost of "down time" analysis to determine which Disaster Recovery alternative makes sense for your business.

Disaster Recovery Options

1. Non-dedicated Standby Server (Off-site)
2. Dedicated Standby Server(s) (Off-site)
3. Failover Server(s) (Off-site or On-site)

Non-dedicated Standby Server

Typically this is the best option for a business with a single server and up to 10 staff reliant on the server to perform their duties.

With this option we install additional software on your server which then allows us to restore a System Backup of your server to one of our Standby Servers (we have a number of Standby Servers available for immediate deployment in the case of a 'disaster' at a client site).

- ✓ On an annual basis (or more frequently at your request) we make a copy of the System partition of your server.
- ✓ We then restore this copy of your system partition onto one of the Standby Servers' in our office to verify the integrity of the System Backup.
- ✓ In the event of a 'disaster', within 48 business hours we will arrange to deliver a Standby Server to your premises with the latest copy of your System partition.
- ✓ Your data can then be restored to make your Standby Server fully operational.
- ✓ The Standby Server is then provided on a rental basis until you have completed arrangements for a replacement server.

Note: For a copy of the full Service Level Agreement, please contact us.

Dedicated Standby Server(s)

Typically this is the best option for a business with multiple servers and more than 30 staff reliant on the computer network to perform their duties.

With this option ZEB host dedicated Standby Servers which are “clones” of your Primary Servers (e-mail, file etc.) at our Sydney office.

- ✓ The Standby Servers do not have to use identical hardware to your corresponding Primary Server as we’re able to “clone” across different hardware platforms.
- ✓ At least nightly imaging software is scheduled to perform an incremental backup, the incremental backup is sent via secure FTP (FTP over SSL) to our Data Centre.
- ✓ In the event of a ‘disaster’, we “activate” the Standby Servers and restore image backups since the last Standby Server restore.
- ✓ We contact your ISP (or other email service provider) and advise them to change the routing tables for your mail, so that e-mail delivery continues to the Standby mail server.
- ✓ Typically the above steps will be completed within 4 hours of you informing us that a disaster has occurred.
- ✓ Once you have organised alternative premises, we can organise to move the Standby Servers to your premises while you organise replacement hardware and re-build your Primary Servers.

Organisations with multiple servers and between 11 – 30 staff will need to assess their ‘cost of down time’ and then make a judgment whether they are best served by Dedicated Standby Servers or Non-dedicated Standby Servers for Disaster Recovery.

For instance if your organisation has 30 staff, 25 of which are customer facing (i.e. billing) and on average they charge at $100 per hour, then every hour of “down time” costs $2,500. If you work on the basis of an 8 hour day, a 1 day outage costs $20,000 plus the detrimental effect on your organisation’s reputation due to the inability to provide service.

Failover Server(s)

Typically this is an option for a business with multiple servers and more than 100 staff reliant on the computer network to perform their duties. Alternatively you may have a high volume Web server generating income 24/7.

Failover Servers provide a "High Availability" option when there is a failure of a key Primary Server at a Site. Failover Servers will replace the operations of a faulty Primary Server in minutes rather than hours, and will do so in a transparent manner (i.e. users will continue to use their applications at the desktop in the "business as usual" mode of operation. For example, they would continue to use their desktop copy of Outlook to access the Microsoft Exchange server).

In contrast to the Level 1 and Level 2 options which are Off-site solutions, Failover Server(s) can either be On-Site or Off-Site depending on the capacity of your WAN links and other Disaster Recovery arrangements that are in place.

Scenario 5

The Head Office is destroyed by a fire or there is a break-in overnight and the servers are stolen.

This is essentially “Scenario 4” except that there is no option to repair the original server as it has been destroyed.

If you don’t have arrangements in place for a Standby Server(s), then you will need to organise new equipment and once that (or they) arrive, start restoring System Backups and the Data Backups as previously outlined. If your original servers used a tape backup system, you will also need to organise a compatible replacement tape drive so that you can restore the tape backups.

Clearly in this scenario, Standby Servers are going to make an enormous difference to an organisation’s “down time”.

This scenario also highlights one of three issues with tape backup systems:

1. That you need a compatible tape drive to restore tape backups;

The other two being:

2. That tapes need to be changed every night;
3. That tapes need to be rotated off-site every night.

This is why our Online Backup System uses disk technology rather than tape.

In the preceding five scenarios we have outlined affordable solutions that address the final two questions posed by ASIC:

- ✓ Do you have a data recovery plan?
- ✓ Do you have a disaster recovery plan?

In conclusion, backups provide insurance against data loss. A business that has good backups will always be able to recover lost files and continue operations.

The need for adequate data backup, data recovery and disaster recovery plans ought to be apparent to all managers; irrespective of whether the organisation falls within the scope of APRA / ASIC regulation or not.