Technical Bulletin: Disaster Recovery

On Saturday February 13th, 2016 at 7:50 AM, Oneir Solutions Emergency Support line received a call. On the other end of the line was Craig Chadwick, President of Chadwick Electric Limited. They had a devastating fire the night before. The successful conclusion to this occurrence is the result of the management and staff at Chadwick, Oneir Solutions and Phil, Chadwick's on-site tech working as a team to implement Chadwick's Disaster Recovery Plan.

Fortunately for Craig, he had the foresight to follow Oneir Solutions recommended procedures and moved his data backup off site.

Effective Data Backup is the first step to your Disaster Recovery Plan

To assist with the commissioning of a new Oneir Solutions Linux server, we have a script that can be scheduled to backup all your critical data, including your company(s) data, the o/s configuration, the users and printer set ups. This backup should be passed over to a storage area where your technical support group would move the backup to a secure off-site location. There should be reporting emailed to company management to confirm that the backup was successfully transferred. Note that Oneir Solutions Inc does NOT store backups of your company(s) data.

If your technical people can extract certain files for us to restore should you need that service, then perhaps our backup files are insignificant – but we had issues in the past where the complete image backup of the server did not enable this sort of extraction – and in one case, that image was not valid and the customer lost a month of data.

Jane Giggal, President of Oneir Solutions Inc said "While this is an uncommon occurrence, all Oneir Solutions customers need to ensure they have the recommend backup procedures in place." Jane went on to say "Chadwick was always vigilant. As a result between Oneir Solutions and Phil, we got Chadwick to a state that they could carry out business when they moved their office to an on-site temporary portable office."

Oneir Solutions Is there to Expedite Recovery

If the server hardware has to be replaced, a new server is required with VMware installed. As with your initial server, Oneir Solutions provides a template consisting of operating system, custom components, Oneir Solutions software programs, network configuration user accounts and printer definitions. Oneir Solutions will also migrate the data from your most recent backup. This process ensures that you are back up and operating with a minimum delay…and cost.

In order to carry out the change over to the new server and get you operating, we partner with your technical people to realize a successful transition. This requires time from the Oneir Solutions personnel to prepare the template for the new server as well as migrating the data and dealing with any unforeseen issues.

Others who are not prepared, are not as fortunate and it costs them weeks, or even months to re-create their lost data. Some companies never recover!

Jane wanted to give one final word of wisdom..."Having a daily backup of your company's data is the cheapest insurance you can buy!" For all those who are reading this article, we all need to ask... What Disaster Recovery Plan do we have in place if this happened to us, or if we simply had a server crash?

Protect Against Server Downtime

In order to minimize the risk of server downtime, some of our customers use dual syncing hard drives, referred to as raid drives, but you cannot ignore issues if they are reported. Some customers have a second server ready to be brought on line, while others simply wait until the server starts showing its age.

Please review these details internally as well as with your technical support group and contact us so that we can ensure you have considered all aspects of your data backup and recovery from a disaster.

_____

Oneir Solutions can set a script to run each night to **create the backup files** of the configuration, programs and data. Moving it off the hard drive to somewhere external is the next challenge.

We can move to a shared Windows folder (smb mount) or if there is a NAS box also capable of having a shared folder, we can script that as well. Obviously we the company's technical group to setup the Windows or NAS side with a user account, password, give us full rights to a folder directly off the root of C: on the other media (Windows or NAS) – that folder name needs to be very simple (I would suggest

less than 8 characters, no spaces, or special characters and I need to have exactly the case of the name as well).

So, in summary for us to set up a share, I need:

- IP of the machine we are moving the files to
- Name of the folder off the root of C: including the case
- A user account and password on that receiving machine that has full admin rights to the folder

Once the files are off the Oneir drive to this external location, they can be incorporated into the Empire's full disaster recovery plan whether that is moving the files to the cloud – or whatever you setup.

A **disaster recovery plan** (**DRP**) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster". The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam, fire or theft).

Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan, sometimes erroneously called a Continuity of Operations Plan (COOP), is increasingly associated with the recovery of information technology data, assets, and facilities. For more details on creating your own Disaster Recovery Plan visit *https://en.wikipedia.org/wiki/Disaster_recovery_plan*

In information technology, a **backup**, or the process of backing up, refers to the copying and archiving of computer data so it may be used to *restore* the original after a data loss event. The verb form is to **back up** in two words, whereas the noun is *backup*.

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss can be a common experience of computer users; a 2008 survey found that 66% of respondents had lost files on their home PC. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required. Every night there is a prescheduled backup of your company data including the configuration files, user setups and printer setups. The Oneir Solutions program files are not backed up as the most current programs can be quickly provided by Oneir Solutions. Your Technical Support Group should automate moving these backups to a secure off-site data storage area by your. There should be reporting emailed to company management to verify that the backup was successfully transferred.

Though backups represent a simple form of disaster recovery, and should be part of any disaster recovery plan, backups by themselves should not be considered a complete disaster recovery plan. One reason for this is that not all backup systems are able to reconstitute a computer system or other complex configuration such as a computer cluster, active directory server, or database server by simply restoring data from a backup.

Since a backup system contains at least one copy of all data considered worth saving, the data storage requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model may be used to provide structure to the storage. Nowadays, there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.

Every backup scheme should include dry runs that validate the reliability of the data being backed up.