May 3,2011

*Delivering Integrated Solutions Since 1994…*

**ESEI is a Telecommunications Engineering and IT services company that designs, builds, and manages networks and systems, with a reputation *for providing outstanding technology solutions through unparalleled customer service*.**

## *Practical Steps to an Effective Technology Disaster Recovery Plan*

No matter how large or small, every business must develop a technology Disaster Recovery Plan (DRP). The DRP must outline what steps will be taken in case the unthinkable happens. The idea of developing a DRP seems daunting, but it does not have to be; below are five practical areas to focus on when planning for disaster:

1. **Identify Threats-** Identify what disasters are highly likely to occur and plan for them. This includes man made or natural disasters. For example; Is the business located in an area prone to floods? What is the likelihood of a fire?

2. **Identify critical business functions or systems-** Figure out what computer systems are critical for the business to continue generating revenue. These systems should be the ones to be restored first.

3. **Conduct a business impact analysis (BIA)-** This exercise will help the business identify and prioritize critical systems and data that needs to be recovered. Some questions to ask are: How long can the business survive without access to data and/or systems? How soon does the business need to be fully operational?

4. **Identify what is in place to recover business critical systems-** The best time to assess if the business is disaster ready is before the disaster occurs. With this in mind, the business needs to ask questions such as: Are there data backups? Are the backups automated or manual? Who is responsible for maintaining the backup process? Are the back-ups offsite?

5. **Identify what can be improved-** Once the business understands what would be available in case of a disaster, existing backup strategy needs to be re-assessed in order to reduce risks.

In general, the cost of downtime is an increasing function of time, i.e. solutions that enable recovery over days or weeks are less expensive that solutions that enable recovery in hours or minutes. It all depends on what

length of time the business can afford to be out of service.

## *Business Technology Language*

As technology changes every day, so does its language. It seems that for any new technical development there is a new "buzzword" attached to it. In our day to day business activities it's difficult to keep abreast of these buzzwords,

especially if you don't feel comfortable with the basics or you just don't use them on a day to day basis. How many times have you been in the middle of a conversation where a "techie" starts talking about the new "Open Source" software they got for their office, or that their cellphone can reach download speeds of 3 "megabits per second" (Mb/s)? Before you start looking for these words and get lost in the cyber dictionaries of Google and Wikipedia, ESEI would like to provide you with some essentials.

**Open Source Software**

Open Source Software is a program that is built on code in the public domain and it is free to use and free to change. Do I use it? You probably see and use open source software every day. If you surf the web with browsers like Mozilla Firefox, you are using open source software. If your company has client or customer databases, it might be driven by the open-source based MySQL.

**Cloud Computing**

Cloud Computing services are web-based services which hosts programs and applications the user needs for his or her job. These programs and applications include word processing, spreadsheet, e-mail, etc. Do I use it? Probably, if you use e-mail services like Gmail and Hotmail, you are using Cloud Computing services. Are there disadvantages to the use of Cloud Computing? Security and privacy could be a problem because your files are saved in a remote computer. Another practical downside is that if you don't have internet connection you don't have access to your files and applications.

**Bandwidth**

Bandwidth is the amount of data bits a device can transfer per unit of time, i.e. 100 MegaBits/sec. The Bandwidth determines the amount of traffic a computer network can move across its connections. Do I use it? Every day, Internet connections are rated based on the amount of bandwidth they can handle, let's say that you have a T1 line running to your business, this transmission media has a bandwidth capacity of up to 1.5 megabits per second (1.5 million bits of data per second).

**Compression**

Compression is the shrinking of a group of files into one smaller block of data. This is often done temporarily so a file can be e-mailed or downloaded faster. Do I use it? If you work with files with extensions such as .zip, .rar, .tar, or .gzip , you are using compression. The downside is that compressed files can be corrupted in the compression and de-compression processes, choosing the right software is the key.

## *Why is My Computer Infected if I have Antivirus?*

Do you keep getting virus infection warnings on your computer? If you do, then you should be careful. Some warnings are true while many are actually fake. How can you distinguish them? Some examples of "pop-up" windows warning the user of false threats may include one of the following:

- **Warning Spyware Threat detected on your PC!**
- **Windows detected Spyware infection!**
- **Your System is in Danger!**
- **Your Computer has Security Problem!**

When one of these pop-up windows comes up, the user needs to refrain from selecting any of the options presented and should turn the machine off. If after

turning the computer on again the problem persists, the user must refer it to his/her IT service provider. Some questions users ask regarding their computer equipment are:

1. **Can my computer get infected if I download a Free Video?**
   *YES: Not only from a Video, also from some other files, especially if your computer is set to hide file extensions, some files are really programs hiding behind a video, word processing, or other type of file.*
2. **Does my computer check for Viruses before I download a file?**
   *YES: If you have an anti-virus program it will scan each file before it is downloaded. Remember, some infections just "prepare" or "open the door" of a computer for later virus attacks. Make sure you have a fully licensed anti-virus program running in your computer; some "free" anti-virus versions only partially protect your computer.*
3. **Can my computer get a Virus if I have an Antivirus?**
   *YES: If you have an antivirus you still can get infected, especially if you download files from questionable sources. Sometimes your computer will warn you about potentially risky files, if you click "YES" on these warnings it is possible your computer will be infected.*
4. **Is my computer better protected if I install two anti-viruses?**
   *NO: There are documented cases where an anti-virus program will block a second program. In some cases, two anti-virus programs can block each other creating an un-protected computer. It is recommended that you have a combination of security layers, a Firewall to protect at the Network level; an Anti-virus program to protect at the PC/Workstation level; and an e-mail anti-spam/anti-virus program to protect at the corporate level.*

***Scan this tag and visit our website!***

***www.esei.com***

***Contact Us Today!***

4141 Pinnacle Suite 208 - El Paso, TX 79912 - Phone: 915-587-7902
www.esei.com Email: info@esei.com