MAKING A COMEBACK:

Everything You Need to Know About Backup and Disaster Recovery

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

TeleConsult Solutions

It is a fact of life that, at some point, any given piece of computer hardware is going to fail. Investing in better quality hardware or designing a system with built-in redundancy can delay or mitigate the effects of that failure, but given a long enough time, failure is still inevitable. If precautions aren't taken, there's a good chance failed hardware will take data along with it.

And for most modern organizations, the data is the business.

This is the reason there is an entire industry devoted to backup and disaster recovery (BDR). There are numerous strategies available to prevent hardware failure from affecting businesses, as well as to help businesses get back up and running as quickly as possible when hardware does fail – or in the case of an equally unpreventable natural disaster.

THE GOOD OLD DAYS WEREN'T

BDR has been around in one form or another since the earliest days of business computing. To call those early strategies BDR, however, is to stretch the modern meaning of the term to excessive lengths.

In the past, BDR typically consisted of physical media backups, generally on magnetic tape, which was then physically moved to a separate location. This is called media vaulting and, as slow and untenable as it would be in a modern context, it was the only option available at the time.

The limitations of this method of backup are immediately apparent. Even though the amount of data being backed up was generally tiny compared to modern business

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

needs, tape drives were glacially slow – the earliest tape drives could only write data at about 7,000 characters per second. There was also the issue of mechanical strain. The tape used in a tape drive was subjected to great stress as it was reeled back and forth in the drive. While the tapes used for business backup purposes were generally very well engineered and manufactured, the possibility of breakage was a real concern.

The biggest issue of all was that even after backing data up to a tape drive, that data was still only present in one other place. Storing the tapes on-site was feasible if the goal was only to protect against accidental erasure, basic hardware failure, or to provide some sort of historical data record, but doing so did nothing when it came to natural disasters such as fires, floods, or earthquakes. In order to deal with natural disasters, the tapes had to be transported to a separate geographical location. This, of course, meant that restoring from a backup in the event of an incident was an onerous and time-consuming process best measured in days rather than hours.

The development of networked computers saw the first major shift in BDR strategies because it enabled the digital transportation of backup data to a secondary location. Businesses were still effectively using off-site media vaulting, but the data no longer had to be physically carried anywhere. Instead, once the backup was performed, the data would generally be transferred over the business WAN connection to the alternate location, where it would be copied to another set of tapes.

This was much faster than physical transportation of data, but still limited and inconvenient. Because those

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

early WAN connections were what today we might euphemistically call “bandwidth-limited”, the backup transfer would either have to happen during off hours when no one else was using the connection, or it would be done at the expense of regular business users who would have to cope with bandwidth that was even more limited than usual.

Off-site media vaulting would be unworkable as the sole BDR strategy in a modern business context. Fortunately, technology has come a long way, and the options available today are much more effective.

ENTER THE CLOUD

The logical extension of the networked off-site media vaulting strategy, of course, is to merge backup with modern cloud computing solutions. The speed of modern data connections combined with the incredibly low (compared to 20 or even 10 years ago) cost of storage means that today, a business of almost any size can avail itself of real-time, continuous backup with a 100% retention rate and almost instant restoration. Data can also be backed up across a nearly limitless array of physical locations, making it as safe as possible from the consequences of natural disasters. Further, thanks to modern encryption methods, it is safe from the consequences of industrial espionage and cyber criminals.

Cloud backups generally work by virtualizing the backup platform across multiple physical storage devices and locations. To the business system it looks like one backup device, but in reality the data is being stored in multiple locations concurrently. The data is often also

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

being backed up iteratively, meaning there are multiple "snapshots" available to restore from at any given time. In the case of a virus or malware attack, it is possible to effectively "rewind the clock" to a time before the attack.

A COMPLEX SYSTEM FOR A COMPLEX WORLD

It may be that, in an attempt to provide a simple overview of the history of BDR, the above may have painted a picture of a simple, unified set of technologies. This, as any business currently shopping for a BDR solution will attest, is not the case. Modern BDR solutions are available in such a wide array of options and methodologies that it can be confusing to determine which options suit the business's needs both now and in the future.

The BDR arena uses a certain amount of industry-specific language in ways that might not be immediately clear to outsiders. Being unfamiliar with the terminology can make it difficult to understand what the options are. Here are some of the more common terms, along with brief explanations:

Disaster recovery: This is the sub-section of network security that concerns itself with protection against data loss and downtime, including loss caused by hardware failure, natural disaster, and even cyber attacks. It is important to note that disaster recovery is not concerned with prevention, but rather with dealing with the aftermath when prevention fails.

Cloud-based disaster recovery: This includes disaster recovery solutions that use cloud-based storage as part of their methodology.

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

Business continuity: This is the planning, processes, and technologies concerned with either keeping a business running throughout an emergency situation, or with getting the business back up and running as quickly as possible afterwards.

Backup and disaster recovery (BDR): BDR is a collection of separate technologies that collectively help protect against data loss in the event of a hardware failure or other disaster. BDR may or may not include cloud options.

Backup window: This is the segment of time allotted for scheduled backups, generally set to occur during periods of minimal system usage.

Recovery time objective (RTO): RTO is the time it is expected to take to restore functionality after a disaster or hardware failure.

Recovery point objective (RPO): RPO is a system of prioritizing data for recovery so as to return a business to operation as quickly as possible after an event. One of the most common criteria used to determine a file's value in a recovery scenario is file age, so this is often used in combination with the system's RTO to decide how often backups should be performed..

A PLETHORA OF BACKUP TYPES

Of the many disparate elements that make up a full BDR solution, perhaps the most important component is the backup itself. Backups come in many varieties, though, and not every type is suitable for every situation. Backup types can largely be divided into full, differential, incremental, and mirror, and those types can further be grouped into local and remote varieties.

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

Full Backup

A full backup involves backing up all files and folders each time a backup is performed. This is, in many ways, the safest backup method – the full data set is available in each backup instance – but it takes up the most storage space and is easily the most time consuming method. Generally, in real-world usage, the first backup is a full backup, which is then followed by differential or incremental backups.

Differential Backup

A differential backup begins with one full backup. Subsequent backups are performed by backing up all files that have changed since the full backup. This provides a much faster backup process, although restores are just as slow, if not slower than from a simple full backup.

Incremental Backup

An incremental backup is similar to a differential backup, but rather than backing up data that has changed since the last full backup, an incremental backup saves only data that has changed since the last full or incremental backup. This means that when it is time to restore, the complete data set is spread across multiple locations. This method saves a great deal of time in backups as well as storage space when compared to either of the previous two methods, but is the riskiest when it comes to restoring.

Mirror Backup

The fourth type of backup is the mirror backup. This type of backup is not simply additive. As the name implies, a mirror backup mirrors the live data set. If a file is deleted in the live set, it will be deleted in the backup, although not immediately. This makes mirror backups the riskiest of the backup types, in particular if cyber attacks are one of the primary threats faced by a business.

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

Most service providers that offer mirror backups work on a 30-day delete. That means that there is a 30-day delay between when a file is deleted in the live data set and when it is deleted in the backup. Although mirror backups are somewhat riskier than the other types and are more susceptible to virus and malware attacks in particular, they do have the advantage of being cleaner and smaller. This can be an important consideration in some circumstances.

All of the above types are available in local and cloud-based versions. A local backup is any type of backup where the backed up data is stored on the business's premises. The storage device might be plugged directly into the machines being backed up or, more commonly, connected to the entire system through the LAN. The biggest drawbacks of this type of backup are the lack of redundancy and the fact that the backup is stored in the same physical location as the original – so in the case of a catastrophic natural disaster, both sets of data are likely to be destroyed.

Cloud-based backups, by comparison, have built-in redundancy and are not located in the same physical space as the original, which provides better insurance against natural calamity. They are also superior in terms of shorter RTO as cloud-based backups often integrate with other cloud-based services, allowing a business to switch to the backup data and continue using cloud-based services with a few strokes of an admin's keyboard.

THE HYBRID SOLUTION

Although hybrid solutions often have the potential to overcomplicate a situation, BDR is a place where hybridization really is the best of both worlds. A hybrid backup plan is, of course, a mix of local and cloud backups,

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

usually involving some sort of NAS device for the local copy and a cloud solution for the remote. This offers the security of remote backups in case of natural disaster, while also providing the ease of use and speed of a local backup. Hybrid backup solutions frequently also allow for the virtualization of servers so that if the primary server goes down, it is a simple matter to get a virtual machine up and running quickly.

THE COMPLEXITY OF BDR

It is important to remember that data backup and disaster recovery are not the same thing. They are closely related and are often dealt with in tandem, but it is important to be able to distinguish between them. It is also critical to be aware of where there is potential for problems in the process.

It is sometimes overlooked that it is possible for the backup software to fail, or for the person responsible for backing up to make mistakes. A backup process designed without consideration for the recovery process is likely to be worthless when it's needed the most – and there is more to the recovery process than simply pressing a button. It is necessary to have the right people doing the right things at the right times with the right tools, and the hardware needs to be set up properly.

BACKUP FOR RECOVERY

Backing up needs to be done with the recovery process firmly in mind. The main reason to back up data is to restore it if something goes wrong. Only by planning the backup process to ensure a smooth and effective (and fast) data

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

recovery in as wide an array of scenarios as possible can a business ensure a smooth transition should disaster strike.

BACKUP IS JUST THE BEGINNING

In addition to having a secure backup of data in a safe location, there are a few other pieces to the BDR puzzle that need to be in place. In part, this means having all of the right hardware and systems to replicate the production environment. Otherwise, it is impossible to properly restore the system after a disaster.

The other half of the puzzle involves the personnel, processes, and equipment needed for the recovery itself. Recovery tends to happen at the worst possible time, when something significantly bad has just occurred. If key people can't be found or vital tools are not available, the whole recovery process can grind to a halt.

WHAT TO LOOK FOR

Ten different businesses looking for BDR solutions would likely come up with ten different solutions. Although they would all differ in the details, there would still be some common aspects that are generally useful for almost everyone.

Cloud and Redundancy

A good BDR provider is one that leverages the cloud to provide redundancy in both backups and, by way of virtualization, service. Make sure that the provider takes measures to ensure recoverability in the case of a cloud service disruption.

Availability

Five nines availability (99.999%) has become the industry

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com

standard, so don't accept less than that. Disasters strike when they strike, not when it's convenient for the BDR provider.

Flexible Pricing

One of the biggest advantages to cloud-based services is their scalability, and BDR is no exception. Look for a solution that can scale as business needs change.

Compatibility

This is often overlooked, but it is important to verify compatibility with the hardware that will be used. Most networks use a variety of devices, and it's important that everything that needs to be covered by the BDR plan is covered.

RTO

How quickly does the business need to be back up and running after a disaster? Can the BDR provider offer that level of service at an acceptable price? Generally, a good BDR provider can measure their RTO in minutes.

PO Box 18686
Phoenix, AZ 85005-8686
Phone: (877) 835-2266
christine.guidi@teleconsultsolutions.com
www.teleconsultsolutions.com