

DISASTER RECOVERY: THE NEXT GENERATION

New ways to help bullet-proof Disaster Recovery plans for companies of all sizes

Submitted by [John Biglin](#), CEO of Interphase Systems, Inc.

When it comes to disasters, companies have two choices: Be prepared, or be prepared to fail. Unfortunately, disasters are not a matter of *if*. They're a matter of *when*. Many people think of major disasters that hit the national news, but there are other types of events that can result in a Total Building Loss (TBL) disaster such as fires, floods, tornadoes, robberies and other events. In fact, we have clients that have experienced one of each of these types of serious disasters.

According to a study by McGladrey and Pullen, every year, one out of 500 datacenters will experience a severe disaster during its operating lifespan. That same study reveals that a full 43 percent of companies who experience a significant disaster never re-open, and 29 percent close within two years. Unless companies have a solid disaster recovery (DR) plan, they are keeping their firm at a serious risk.

Over the past several years, a technology known as Virtualization has emerged as an easy and reliable way to improve disaster preparedness. This technology provides companies the ability to dramatically increase the efficiency and availability of their resources in the event of a disaster. Using virtualization, companies can ensure they are back online within minutes or hours, rather than days, weeks, or months.

WHERE TRADITIONAL DR PLANS FAIL

In our experience, nine out of ten companies—from small businesses to multi-billion-dollar corporations—are not prepared to recover from a fire, flood or other major disaster. Their DR plans are either weak or non-existent.

Here are some of the most common problems we find with traditional DR plans:

Many are half baked. Some DR plans are sitting in “draft one,” meaning they are incomplete, inaccurate, and outdated. This can occur when companies take the “big binder” approach. They assemble a large document outlining a DR plan. But if they do not complete it or update it as their IT environment changes, it quickly becomes invalid. For example, some companies create a DR plan because an audit is coming down the pike. Since they are usually short on time or resources, they tap whoever is available, including lower level personnel or interns, to create the plan. That can be a big mistake. Without a seasoned and experienced team dedicating the appropriate amount of time to developing and testing the plan, the result can often be a half-baked strategy that is useless in a real disaster.

The plan is untested. An untested DR plan is equivalent to not having one at all. Numerous barriers can prevent companies from creating test plans. First, some companies do not even realize they need a test plan. However, testing is crucial for ensuring DR plans will truly work. Or, too many people are involved in the decision-making process and the team cannot reach an agreement on the plan's contents.

Sometimes we are told that an IT leader has much of the plan “in his head”, which is an obvious significant risk for the company. DR plan testing is a requirement, not an option.

Recovery tools do not always work as expected. Certain recovery methods or tools can also be faulty. For instance, backup jobs might not be capturing every file. This can occur if the backup configuration is outdated. Say it’s set to capture 200 directories on a server, but 100 more folders have been created since the backup job was originally created and configured. Obviously, those 100 folders would not be captured if the backup is not updated appropriately. Sometimes backup tapes have deteriorated from age and overuse. This prevents companies from restoring the data that resides on those tapes. Sometimes we see the discs and license keys for the backup and restore software are saved on or near the server. So when the data center collapses, companies cannot access the software or its installation keys to install the recovery software in order to restore backed up applications and data.

Not all Outsource Partners are Prepared. While many DR partners provide adequate recovery services, some DR partners may not be prepared for real disasters. They can be slow to respond, and lack the technical wherewithal to recover systems and data for multiple clients simultaneously. We have seen this many times. Some organizations assume their hosting provider has everything covered. Just because they are a big name or have a big data center does not mean that this is always the case. We have seen many cases where hosting providers are unable to test a DR plan for client environments. Unfortunately, some companies find this out the hard way, after disaster strikes. In the end, you are responsible for your firm’s recovery, whether you manage it yourself or engage a partner company.

Recovery and production systems are incompatible. With traditional physical IT DR plans, recovery systems must often match the production environments identically. Most hardware and software components must have the same general model, configurations, etc. Again, when a component of the production environment is changed or updated, it must also be updated in the recovery environment. This can become a costly, laborious and time consuming resource drain.

VIRTUALIZATION OFFERS SOLUTIONS

Companies are increasingly abandoning their old DR platforms, and turning to virtualization technology to prepare their business for disaster and safeguard their assets.

The technology fundamentally changes the way back-end system resources are accessed and utilized. With regard to DR, a virtualized environment lets companies take snapshots of their servers, desktops, and other components and store them on a storage area network (SAN) or other storage media. These snapshots are part of the virtual environment, which can then be restored to another data center location that has been equipped with virtualization technology. In some cases, environments can be replicated so that no restore is necessary.

Virtualization can help companies establish a highly reliable DR plan to greatly mitigate the impact of a disaster in several ways:

Break the hardware dependency. Virtualization allows companies to transform physical servers into virtual machines, which reduces dependency on multiple physical resources. There's no need for one-to-one hardware duplication because the hypervisor handles all communication between the virtual machines and the resource pool hardware. As such, the physical setup in production can be different than at the recovery site. Additionally, as companies upgrade their physical servers, legacy servers can be used to host recovery systems. This saves the cost of new recovery hardware.

Increase server portability. Virtual servers are much more portable than physical ones because they essentially become a set of files that companies can copy to tape, DVD, etc. and restore like any other file. In the event of a disaster, files can be loaded onto any server running a compatible hypervisor. From that point, with the appropriate network changes, the protected systems could be up-and-running within hours, instead of days or weeks. Companies can also easily take the files to an outsource partner for testing.

Nearly eliminate planned down time. Planned down time, including hardware maintenance, software updates, etc., typically constitutes 80 to 90 percent of all down time. Virtualization allows companies to significantly reduce or eliminate this downtime. Virtual environments can be dynamically and rapidly moved to different physical servers within a resource pool without interrupting the business. While maintenance is performed on one physical server, employees can continue to work on their virtual servers that are running elsewhere in the resource pool, thereby eliminating downtime for the maintenance.

Test rapidly and keep it current. Virtualization allows companies to take snapshots of their production environments and store them on a storage area network (SAN) or other device/media. DR plan testing can then be done on these snapshots, which eliminates the laborious build, install, and restore process typically required for traditional DR testing. This reduces several aspects of the testing process, including its complexity, the number of specialized staff required, propensity for human error, and cost. By using recent snapshots of the production servers, companies can be assured that they are testing the most current system configurations as opposed to maintaining recovery site configurations, configuration manuals, etc.

Be mobilized for disaster. Depending on how the environment is architected, Virtualization lets companies enable their recovery sites within minutes or hours of a disaster, rather than days or weeks.

In addition, some virtualization platforms offer a tool that automates certain DR steps. These might include pausing non-mission-critical servers, halting replication, launching specific servers in a set order, bringing storage components online, executing DR tests, and documenting results. This reduces human error and ensures systems can be rapidly recovered in a repeatable and reportable fashion, rather than relying on a 400 step run book binder.

Create virtual desktops. Data center recovery is a primary part of DR. But many companies overlook another important aspect: desktop recovery, which is vital to accessing the restored datacenters. Virtualization can meet this need by providing a mechanism for companies to create and store virtual desktop snapshots. By configuring

an appropriate remote connection to a recovery site, companies can manage virtual desktops from a central datacenter, and employees can load and access their desktops, as well as the recovery site, from any physical machine.

Don't forget about Phone/Voice Services DR. Just like many firms forget to address Desktop Services in their DR plans, a high percentage also don't think to plan for recovery of their Phone Systems. With today's Voice over IP (VOIP) technologies, it is reasonably easy to include so called certain phone systems and voicemail in your DR Plan.

Available for Small, Medium, Large and Enterprise size Companies. Historically, only multi-billion dollar organizations could afford rapid, repeatable and comprehensive enterprise disaster recovery. But today, DR is affordable for companies of almost any size who leverage virtualization technology. With vendors offering a multitude of options and packages, companies can tailor their virtualization strategy to their IT environment and budget.

The key to an effective DR plan is proper architecture, planning and strategy. The right strategy can provide companies greater flexibility in managing their environments, creating a solid foundation for balanced, stable, and continuous operations. With virtualization, companies have a way to create the strongest DR platform to protect their business and assets from disaster.

About the Author:

John Biglin is the CEO of Interphase Systems, Inc. He is also an accomplished writer, speaker, advisor and professor and is a member of several corporate Boards of Directors advising executives in areas key areas of strategy, compliance and technology.

About Interphase Systems, Inc.

Founded in 1995, Interphase Systems, Inc. is a premier management and technology services organization providing architecture, development, strategy and implementation services to various industries across the country. With three distinct practice areas, Interphase specializes in all aspects of Enterprise Architecture, Regulatory Compliance, and Strategy Services. Interphase also provides outsourced managed Disaster Recovery and Application Hosting services for its clients. For more information, visit www.interphasesystems.com, e-mail info@interphasesystems.com or call (610) 276-5500