Business Continuity:
Considerations, Risks, Tips and More

Table of Contents

Additional Reading

ITBUSINESSEDGE

Five Key Considerations for Backup and Recovery

All enterprises need reliable, efficient data protection and recovery – it is fundamental to business survival. In recent years, mid-sized businesses and distributed enterprises have been largely underserved by data protection hardware due to its high cost at a time when enterprises struggle to keep up with the rising tide of data. While hiring a full-time resource dedicated to managing data backup may not be feasible for small and medium enterprises (SMEs), many software packages, appliances, target arrays and services provide comprehensive data protection and recovery. Mason Swenson, product marketing manager for Imation's Nexsan solutions, offers five important considerations specifically for SMEs when evaluating their data protection needs and plan.

Consideration #1: Backup Speed

How quickly and efficiently can data be backed up? When an appliance is first added to the system, the first complete backup will take some time. However, once the first backup is complete, updates should take only a few minutes each day, and be virtually unnoticed by end users on the network, assuming business-grade network connectivity is in place. If a slow backup causes a general network slowdown for end users, IT might be forced to suspend backups, completely derailing the data protection plan.

Consideration #2: Recovery Time

Backup speed is important but recovery speed is where the data protection plan proves its worth. In the event of a system crash or disaster, how fast can critical data be recovered and accessed? Businesses should establish a recovery time objective (RTO) and a recovery point objective (RPO). RTO is the time by which a business process must be restored after a disaster or disruption to avoid unacceptable consequences of a break in business continuity. RPO is essentially the minimum frequency of backups – which translates to the amount of time and data that would be acceptable to lose in the event of a disaster.

By establishing an RTO and RPO, a business can maximize business continuity by creating a tiered data protection system that ensures the least possible loss of the most important data.

Consideration #3: Reliability

How reliable is your backup and recovery ecosystem? Once you define the strategy, it is critical to implement that strategy on an infrastructure you can trust. By ensuring both best practices and high-quality, reputable storage hardware and software systems, the organization can be confident that backed up data will be there when it needs to be recovered.

Consideration #4: Simplicity

If the data protection strategy and systems are not easy to implement, you risk mistakes or missed backups at critical times. Additionally, ease of use and management capabilities are critical for evaluating long-term resources necessary to maintain an effective strategy, especially when IT resources are limited or outsourced. While some technology platforms may be more affordable, an administrator’s time to monitor could add significantly to cost. Look for solutions that enable storage administrators to set policies so that backups run seamlessly without much need for interaction.

Consideration #5: Cost Efficiency

What is the cost – not just to acquire, but also to operate? Key total cost of ownership (TCO) considerations include energy efficiency, maintenance, and scaling up the system to manage data growth. A tiered storage strategy is critical here. Tying storage system performance and cost to the value of the data, and quickly moving fixed content and other non-production information onto reliable, lower cost systems will help manage cost while delivering on the access level and recovery time objectives required.

Additional Resource

Disaster Recovery Training Outline

Your team needs to know in advance which data and applications are most critical to restore in case of disaster or other large-scale system failure. This guide will help get them prepared.

Download Now

The Seven Deadly Sins of Backup and Recovery

From storms like Hurricane Sandy to component failures to human error, there are myriad situations and emergencies that can threaten an organization’s data, servers and systems. Businesses of all sizes need to make sure their business continuity/disaster recovery plans are up to snuff, so as to minimize downtime, preserve customer service and prevent the often-dire ramifications of data loss.

Having a comprehensive disaster recovery plan doesn’t have to be an elusive goal, though there are common and, unfortunately, crippling mistakes that organizations often make. Based on its experience in the field, Unitrends, a provider of all-in-one backup, archiving, instant recovery and disaster recovery solutions, has identified the seven deadly sins of backup and recovery in the hopes of helping companies avoid a fatal failure.

Organizations, beware: This article features the perilous pitfalls, including information on how and why they happen and, most importantly, how they can be avoided and overcome.

Deadly Sin #1: Backing Up Data Only

It used to be that backing up only user data was the norm for virtually every organization, but today – with significant risks at the operating system (OS) level – that's a dangerous mindset. Your data protection processes should include not only backups of user data, but also backups of the OS layer and all applications – along with the ability to quickly restore and recover each.

Additional Resource

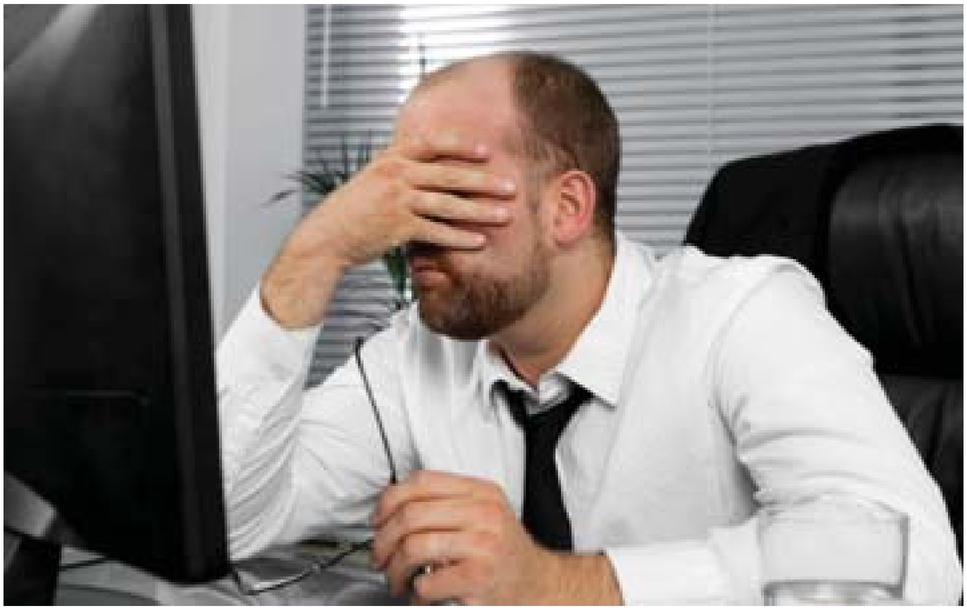
Job Description: Disaster Recovery Administrator

In addition to designing processes for re-establishing failed systems, a disaster recovery engineer must also run simulations to ensure those plans will work when it matters most.

Download Now

Deadly Sin #2: Allowing Backups to Go Untested

Organizations often spend an enormous amount of time making backups. However, if the backup volumes can't be restored on a reliable basis, the process has effectively failed. Don't be caught by surprise when it's too late. Instead, make sure your backups are



performing correctly and incorporate redundant backups into your disaster recovery plan to compensate for normal error rates. The change rate of your data is a good benchmark to determine how frequently you should test your backup process.

Deadly Sin #3: Lack of Adequate Recovery Planning

Most IT organizations have at least some level of a “plan” to address a serious IT failure or natural disaster. But these plans often lack specificity and fail to lay out a roadmap for a successful recovery in the event of different kinds of disasters. It’s important you tailor disaster recovery plans to address various scenarios and use technologies capable of backing up your whole IT infrastructure.

Deadly Sin #4: Not Planning for Dissimilar Recovery Environment

We tend to think of laptops, desktops and servers as nearly universal devices, and, as such, organizations often don’t consider the risks and complexities of moving software and data between different brands or models. At the same time, they often assume that if there’s a failure and a need to shift to new hardware, they’ll be able to quickly acquire whatever they need. But beware, system driver, application and patch complexities and incompatibilities can undermine the best laid plans. Your organization should think about these issues in advance, and plan for realistic restoration choices in the event of a disaster.

Deadly Sin #5: Not Having Offsite Copies

With software security threats (such as viruses, malware, etc.) often grabbing headlines and executive attention, organizations can sometimes overlook the importance of physical security. Surprisingly, many companies do not have a formal, secure process for regularly taking backup copies to a remote location, but this is important as a way to combat and recover from natural disasters, on-site mishaps and theft, and also to comply with industry-specific legislative requirements.

Additional Resource

Disaster Recovery Training Outline

Your team needs to know in advance which data and applications are most critical to restore in case of disaster or other large-scale system failure. This guide will help get them prepared.

Download Now

Deadly Sin #6: Confusing Replication and Vaulting

Replicated disk storage offers benefits including near real-time data protection, as well as ease of configuration. However, drawbacks include the fact that synchronization occurs at a low level, causing errors that naturally occur over time to be immediately replicated

to the offsite location. In addition, replication is often resource- and bandwidth-intensive, taxing the corporate network infrastructure. An alternative, preferable approach to offsite data storage is called “vaulting” – allowing for a level of file system integrity not found in a replication environment. It’s also a best practice for IT professionals to look for a vaulting system that moves only changed data to minimize bandwidth requirements and maximize backup windows.

Deadly Sin #7: Adopting Inflexible Solutions

Often, the only certainty in backup and disaster planning is that the post-disaster environment will be at least somewhat different than what was expected and planned for. As a result, it’s important to select solutions that incorporate natural flexibility. For example, the ability to restore to a virtual machine environment gives your IT leaders intrinsic choices. By picking a business continuity solution that accommodates the majority of the needs you’ve already identified – plus others that may not be in today’s plan but could still be useful – you’re well on your way to being back in business quickly.

How to Maintain Operations During a Regional Disaster

This article features a checklist, developed by SunGard, of high-level tasks that should be considered in threat or response mode. Topics range from assessment and plan activation factors to safety issues, security, communications and personnel notification guidelines. While not a substitute for a comprehensive incident management plan, the checklist provides a concise overview of key areas to address. An expanded version of this checklist can be obtained on request from SunGard Availability Services.

Tip #1: Threat Response

If there is a high probability of an event occurring, consider the following:

- Identify incident management team members, including an incident manager, and alternates.
- Identify business and information technology recovery team leaders and alternates.
- Update all critical internal and external contact lists. Include home address, home telephone, cellular phone, pager, and email address.
- Establish a conference bridge. Provide all incident management team members the conference bridge number and pass code.

- Establish a voice mailbox for employees to monitor for status updates.
- Determine if you should place SunGard on alert if you are a subscriber (see SunGard Alert and Disaster Notification Procedures).
- Ensure that monitoring service vendors (e.g., alarm company) have current contact information.
- Develop procedures to account for employees.
- Provide employees with threat response procedures, if appropriate (e.g., bomb threat, evacuation).
- Create backup tapes and ship off site.
- Identify a crisis command center outside of the anticipated impact area.
- Top off emergency generators and arrange for additional fuel deliveries.
- Acquire battery operated radios with spare batteries.

Tip #2: Incident Detection and Preliminary Assessment

- Follow company emergency response procedures
- Conduct a preliminary damage assessment, if it can be done safely. No recovery activities should be undertaken if personnel are placed in danger.
- Notify the incident manager and provide a detailed report.

Tip #3: Activate Incident Management Team

The incident manager will determine if the incident management team should be activated and if necessary:

- Notify incident management team members to provide a description of the event and request that they assemble at the crisis command center or participate via a conference call.
- Activate the crisis command center.

Tip #4: Evaluate Disaster Impact

- Determine if the severity of the impact requires implementation of the recovery plan.
- Determine recovery objectives, including priorities, recovery strategies, action plans and assignments.

Tip #5: Activate Recovery Plan

- Notify recovery team leaders and members.
- Brief recovery team leaders and alternates regarding priorities, strategies, action plans, assignments and reporting and communications procedures.
- Declare a disaster with SunGard if you are a subscriber.

Tip #6: Implement Support Procedures

As directed by the incident manager, incident management team support personnel will provide recovery support to all affected business units. Checklists for individual business units can be obtained from SunGard Availability Services.

Seven Reasons Why Companies Need to Automate Disaster Recovery

Data and IT services make up the lifeline of any modern business enterprise, large or small. Before a data center fault occurs — either one caused by human error or a natural disaster — executives want to be assured that their data is secure and protected. Executives know that downtime equals lost dollars and that every minute spent on recovering data and systems is time taken away from running their business. This results in lack of productivity and poor customer response time. Companies can create a resilient IT infrastructure with automated disaster recovery (DR) for any service, any time and any place. This slideshow features seven reasons why companies need to automate disaster recovery, as identified by Ralph Wynn, senior product marketing manager at FalconStor Software, a leader in data protection and DR.

Reason #1: Tradtional DR Plans Require Too Many Steps

Traditional methods consist of hundreds of steps to recover data and applications. IT staff is often required to reboot servers, applications and infrastructure. Should an error occur during the process, the complete recovery may take twice as long. To address these issues, companies are turning to replication and automated technologies for DR, since they eliminate these complex steps by automating them.

Reason #2: During an Outage, Business Operations Come to a Halt

Data and applications are at the forefront of any company, and without them business processes suffer. Companies want to ensure that their websites are operating properly and are allowing customers to access information. When the data center fails, customers can't research services or purchase products, the sales team can't access details on potential customers, finance is unable to balance the budget or distribute checks and reports are lost.

Reason #3: IT Cannot Predict When These Issues Might Occur

We are often alerted if a natural disaster is expected to strike, but we can't predict other causes of data center failures. Outages can be the result of malicious acts or simple human error. Data protection systems employing replication and automated DR solutions enable IT administrators to build resilient infrastructures that will keep data and applications accessible during outages and avert downtime.

Reason #4: Providing Data Protection and DR Services for an Entire Infrastructure Is Challenging

Companies face a surge in data growth, hybrid environments and limited budgets and staff. However, data center professionals must ensure they have an insurance policy — also known as a disaster recovery plan. Automated DR and data replication solutions keep data centers functioning around the clock.

Reason #5: Disaster Recovery Planning Is More Than Just Backing Up Data

The value of automated disaster recovery is that it can recover complete IT services at once. Services are made up of data, files, applications, servers and other components. If a data center

Additional Resource

Job Description: Disaster Recovery Administrator

In addition to designing processes for re-establishing failed systems, a disaster recovery engineer must also run simulations to ensure those plans will work when it matters most.

Download Now

manager only restores data and the application on which it resides is not available, the data is useless. Data center managers must look at DR from an IT services point of view.

Reason #6: Automated DR Recovers Systems Without Human Intervention

IT staff can initiate a carefully designed and tested automatic DR process with the click of a mouse. A fully automated DR system will initiate a series of actions in a precise order that reinstates one component after another until the complete service is on line – eliminating time-consuming manual procedures.

Reason #7: Automated DR Provides Data Center Managers with Peace of Mind

With automated DR, IT staff can avoid late night calls about outages that have made customers angry. Automated DR eliminates stress and saves countless hours, so data center managers can focus on more strategic projects. Rather than looking for lost files that someone may have accidentally deleted, data center managers can put out numerous fires with ease.

How to Stay in Business:
Key Considerations for Disaster Recovery

In the wake of the increasing threats to the data center via cybercrime and the recent natural disasters occurring across the globe, AFCOM's Data Center Institute believes it is time to review the adequacy of existing data center business continuity and disaster recovery plans.

They maintain that the cloud offers new and dynamic approaches to the art of disaster recovery. It builds upon the techniques developed with load balancing, virtualization and geographical separation of assets. If done right, the cloud can drive multi-purpose utilization of assets, which makes disaster recovery more affordable and can provide significant ROI.

Leveraging the cloud for use in a disaster will require pre-planning and monitoring of the resources available in the cloud to ensure that what's needed is there when it is needed. This slideshow features eight key steps, identified by AFCOM, for taking advantage of the cloud for disaster recovery.

Step 1: Assign a Leader

Perhaps the most important component in running DR within the cloud is to assign a leader to design and manage the environment. The complexities associated with building and managing this environment are deep and overarching. Coordination between application owners and data center managers must be planned and executed with precision to guarantee success. A strong leader with the authority to set the direction will be an imperative.

Step 2: Standarize Platforms

Standardization of the platform is important in reaping the benefits of the cloud. Having standard hardware, processors, OS versions and builds make transporting virtualized containers easier and more reliable. Choosing a platform is something that must be done in partnership with both the application architects and the data center managers. Having a mismatch will result in applications not porting into the cloud during critical times.

Step 3: Prioritize Applications

Application prioritization is traditionally necessary to determine which applications get first access to available CPU cycles during the recovery process. In the cloud, resources are infinitely available, but you must still prioritize the order of application deployment to ensure the most critical systems are up and running first.

Step 4: Replicate Data

Using traditional methods of data replication comes with a list of issues such as latency, mean-time to restore data and offsite storage. In the event of a disaster, your data is only as current as the last backup. Tapes must be shipped from the offsite storage location and then restored at the DR site. This can take days or weeks depending on location and disaster preparedness.

With cloud computing, new products are coming on the market every day to help create mirrors of data that are dispersed across cloud domains. This mirroring in effect protects the data from any single point of failure and removes the need to replicate data in a static fashion. As application traffic is transferred to other areas in the cloud the data is there to support them with limited disruption.

Step 5: Route Network Traffic

Network traffic routing and capacity in the cloud can be confusing and complex as cloud providers try to make it abstract and simple to manage. Some providers even claim that the network is invisible. The most important aspect is to make sure that the cloud provider, whether private or public, has enough bandwidth to support all of its customers. In catastrophic events such as 9/11, many DR facilities found themselves short of network capacity since they oversold their service.

Monitor your network usage across the cloud and see what levels are reached during peak times. Add all of the usage together across the cloud and determine if your hosting locations can accommodate the increased usage if any portion of the cloud goes out of service.

Some providers will allow you to pay more to be placed in higher priority slots (above other customers). Make certain you address these issues before committing. Another trend to investigate is cloud balancing, where you are leveraging multiple cloud providers to keep your applications highly available.

Step 6: Monitor and Oversight of Application Architectures

Monitoring and oversight of application architectures will make certain you have what you need in the event of a disaster. If you are using the cloud as a DR site for hosting your application, ensure that all application changes are implemented in your cloud provider accounts. Any changes to the hardware or OS in one private cloud facility must be planned and replicated at the disaster site. This is a key advantage over traditional DR facilities where they may sit idle and quickly become outdated and unable to support the applications. New products today simplify how to electronically replicate your application environment in the cloud, across domains.

Step 7: Address Security Concerns

Implementing public, private or hybrid clouds raises many questions and security concerns. Can you trust the security of your data authentication, access control, encryption and monitoring? Protecting the data itself and/or access to the database are both areas of concern. Several methods exist including standard encryption tools and tokenization. Investigate the best solutions available by discussing it with your database tool provider. Whatever solution you choose, be aware that application performance can be impacted so make sure to balance risk against performance.

Step 8: Follow Goverment Regulations

Lastly you need to understand where the data is ultimately stored. Several countries have governmental regulations that do not allow certain data to leave the country. Make certain that the data is categorized and assessed against regional data protection policies. Some cloud providers offer selectable geographical zones for CPU and data location.

Additional Reading

Keeping Disaster Recovery Plans in Tip-Top Shape

Arthur Cole, Infrastructure

Disaster recovery is one of those IT functions that can never be fully completed. No matter how good you think your program is, it can always be made better. And the fact that its worth cannot be proven except when confronted by extreme circumstances makes it difficult to devote time, money and resources to the cause.

Yet that's exactly what is required on a regular basis. As Forrester's Rachel Dines pointed out recently, DR is the equivalent of running a marathon - only those in tip-top condition will see the finish line. Unfortunately, virtually no one out there runs a full DR test even once a year. At best, organizations test individual components to ensure continuity of various application subsets, mainly out of fear that more comprehensive trials will upset ongoing business processes.

And that's only among organizations that have DR plans to begin with. And the fact is that too many enterprises are still without a means to recover from even minor disruptions let alone the kinds of calamities that make the evening news. The cloud has proven to be a friend in need for groups that can't afford backup data facilities and advanced DR platforms, but there are still many pitfalls when it comes to maintaining continuity in the cloud. As CSO's Gregory Machler notes, many firms make the mistake of striving for broad load balancing among public and private resources so that no matter what happens, there will always be resources available from somewhere. This is trickier than it sounds, however, as applications tied to specific servers, IP addresses, DNS mappings and the like will likely crash if the underlying infrastructure were to suddenly shift. A much better solution is the hot-cold data center approach so transitions can be charted out ahead of time.

The cloud's chief advantage, of course, is scalability, which allows companies to ramp up DR resources without breaking the bank. Lately, attention has shifted toward integrating these massively scalable solutions with the often heterogeneous server, storage and networking environments that exist in many enterprises. A company called InMage, for example, has tailored its vContinuum system to provide a cohesive environment across Windows, Linux and UNIX servers coupled with DAS, NAS or SAN storage. The idea is to provide block-level asynchronous replication of VMware virtual machines with little or no disruption to production servers.

At the same time, in-house DR technology is becoming cheaper and easier to deploy. Veeam Software has tapped SAN developer Coraid to create an integrated data protection, disaster recovery and management solution that can be deployed at a fraction of the cost of traditional Fibre Channel systems. The system combines Coraid's massively parallel 10 GbE EtherDrive and Veeam's Backup & Replication system to enable vSphere and Hyper-V off-site replication and rapid recovery, utilizing source-side deduplication to limit file size even as overall capacity scales into the petabyte range.

This probably isn't the first time, nor will it be the last, that someone tells you disaster recovery is too important to push to the back burner. But as both cost and complexity of DR solutions continues to diminish, so too will the institutional resistance to establishing a comprehensive program. Once in place, however, it will be up to IT to ensure it sees regular testing and updating as data environments evolve.

Don’t Dither on Disaster Recovery/Business Continuity

Carl Weinschenk, Mobile and Telecom

Friday’s frightening commuter train crash in the Connecticut suburbs of New York City is another example that things don’t always go as planned.

Few people disagree with the rationale behind disaster recovery and business continuity (DR/BC). Indeed, DR/BC seems to be getting more important as time passes -- the emergencies get more severe and downtime more disruptive and costly.

The problem is that there are dozens of different ways to handle DR/BC. From maintaining up-to-date lists of employee cell phone numbers to using the cloud, almost anything an IT department does – if done carefully and with redundancy built in – arguably is DR/BC. That’s great in a way: By using certain best practices, a company can integrate BC/DR into its normal way of doing things.

But it also is confusing. The questions become: If everything is BC/DR, what is it, exactly? Where do we start?

CIO Insight has a nice slideshow up outlining 10 vital steps – ten commandments, they call them -- that provide that starting point. Here are the first five: Eliminate single points of failure; keep “notification trees” timely; follow current events, from impending storms to heightened terrorist threats; keep an eye on many areas within the business that could lead to problems as possible and document the steps to recovery so that they can be performed by secondary staff if the person who usually would run the show is not available.

The cloud – which by definition distributes intelligence – is the best thing to happen to DR/BC since the invention of the cell phone. SunGuard, one of the big names in disaster recovery, is positioning itself to use the cloud as a conduit for its services. The Network World piece details the company’s plans, which seem to be incomplete or only partially public. The bottom line is that SunGuard understands that companies are moving their data to the cloud as a sort of do-it-yourself DR/BC solution. That’s a great opportunity for the company to offer cloud services that are combined with its unique DR/BC background.

A more academic look at DR/BC is available at The Metropolitan Corporate Counsel, a partner in the Litigation and Corporate Financial Advisory Services Group at Marks Paneth & Shron

LLP, writes that companies must consider whether to invest in a comprehensive approach or to simply protect its data:

> Risk can be limited to data security or be widened to encompass operational issues should a major disaster actually occur. While the costs of a complete disaster recovery plan will be much greater than a plan designed solely to protect lost data, the consequences of one versus the other should, at least, be considered by management.

There are ideas available on the key of where to start and how to approach BC/DR. The bottom line is that a lot of things fit into the definition of business continuity/disaster recovery. Businesses that have not paid attention to this important part of their ongoing operations must determine what for them is the best place to start. The time to opt out because the topic is too confusing or expansive has passed.

Creating a Disaster Recovery Plan for Your Small Business

Paul Mah, SMB Tech

Putting together a disaster recovery plan isn't something that is reserved to the domain of large or enterprise businesses. While the endeavor can indeed be a complex undertaking for bigger organizations with thousands of employees, a small business or SOHO (some office, home office) can probably put together a working disaster recovery plan in relatively short order.

With this in mind, I outline some of the most important areas and suggestions on disaster recovery below.

Back up Work Data

The most precious asset of a typical business these days would probably be its digitized data. As such, any disaster recovery plan necessitates that a copy of this data is regularly achieved at a location that is not only geographically separate, but also easily accessible.

One method of fulfilling the two prerequisites specified above would be to rely on a cloud storage service such as SugarSync. Businesses are well advised to carefully consider the relative risks of storing unencrypted data in the cloud, which does carry inherent risks not found in backups that are stored offline. For now, you may want to check out my "Three Methods of Backing up Your Crucial Work Files in 2013" for more information on backing up your work data.

Restoring Server Assets

Having a backup copy of data on hand is good, but of little immediate use if replacement servers required to make use of them cannot be deployed within a reasonable timeframe. As it is, remember to make a full image of the operating system and supporting software on a regular basis using server backup software such as Acronis Backup & Recovery.

It is for this reason that many businesses have opted to fully virtualize their infrastructure, which allows them to make copies of the entire virtual machines with little effort. If done properly, these software virtual machines can be copied onto a replacement server and reused with little configuration needed. Obviously, making use of cloud infrastructure and online services offers the same benefit; though it is worth noting that even Amazon EC2 is known to fail.

Working from Home

The earlier two points address the ability for small businesses to restore their work data and infrastructure in the wake of a disaster. Moving ahead, the next consideration is being able to resume work with the shortest amount of interruptions, or to continue working while waiting out inclement weather, for example.

For this to work, employees need to be prepared to work from home, preferably armed with company laptops. This does also entail the availability of speedy broadband access, as well as some means to securely access the work files once they are recovered from data storage and redeployed on new servers.

While the above areas are what I consider to be the most important aspects, it is important to remember that the finer details of how a small business can get up to speed will obviously differ from one business to the next. The above pointers should be a good start for just about every small business, however.

The Role of Virtualization, Recovery Testing in Disaster Recovery

Paul Mah, SMB Tech

I was reading a report about how a mid-sized firm successfully slashed the backup window for restoring its SQL database from 17 hours to just two. Titled “How One SMB Slashed Disaster Recovery Time,” it was an interesting piece about how wholesale distributor Hit Promotional Products dealt with the massive and increasing load of data that the 10-person, developer-centric IT team had to work with.

I thought that some of the insights shared by CIO Eric Shonebarger are relevant for small-sized businesses as well, especially where it pertains to disaster recovery.

Virtualization for Easy Disaster Recovery

Hector Lariveé Boosts Infrastructure Capabilities and Uptime
Download Now

According to Shonebarger, the company stumbled into virtualization when it deployed an extra server as a host to test out virtual machines. As the number of virtual machines grew, the company decided to make an investment in an EqualLogic SAN, anchoring its virtualization strategy around a VMware environment for all its servers with the exception of its email system.

Though it wasn’t mentioned, the virtualization of physical servers into virtual machine packages undoubtedly contributed to an easier time in terms of system backups and disaster recovery. For unlike physical servers, digital copies of virtual machines can be easily made and restored - given adequate storage resources.

Time Taken for Disaster Recovery Matters

The strategy of retrofitting existing technology and processes into a virtualized environment is not a perfect one though, and can lead to its own set of problems. By treating virtual machines like physical machines, the company soon realized that managing a large virtualized infrastructure may require new tools given the likelihood of entire virtual machines being erased by mistake.

Specifically, Shonebarger came to the realization that a complete restore of the company’s infrastructure from backups would take days - hardly tenable in an era of cloud computing and always-on connectivity. After some exploration, the company eventually settled on Veeam as its backup and recovery tool of choice. While the road taken by Hit Promotional Products may or may not be suited for a particular SMB, the takeaway here is simple enough: Disaster recovery takes time, and businesses should take into consideration the amount of downtime that their business can tolerate. This can be used to establish realistic recovery time objectives (RTO), which I wrote about in “SMBs Should Approach Disaster Recovery Differently.”

Recovery Testing

“Don’t confuse high availability with backup and recovery,” Shonebarger said, underscoring the importance of data backups as opposed to focusing only on high-availability systems. On this front, Shonebarger advocates recovery testing, which is when a company simulates a data recovery by performing a recovery according to documented procedures.

Admittedly, the amount of resources and time required for a small business to perform recovery testing can be significant. It is important, however, that SMBs understand how this can help catch loopholes or flawed procedures in the advent of a total IT failure. After all, what good is it to establish a backup regime when not all data is recoverable in a disaster?

Let Risk Management Team Carry Part of the Disaster Recovery Planning Load

Kachina Shaw, Governance and Risk

Disaster recovery planning has long been a hot topic on IT Business Edge, with the main focus on systems and service continuity, customer service and data preservation. But what is often glossed over is that, alongside the infrastructure/DR team, the risk management officer or team should be involved from the beginning planning stages. Unfortunately, DR sometimes tends to be handed off to IT, as if it can be planned and carried out in isolation, and the rest of the company needn't worry as long as they've got the IT on-call number when everything blows up. The good news is that the end result will be stronger if the larger IT group doesn't try to carry the entire load alone.

It's true that disaster recovery planning is a complex balancing act of priorities for IT. What your risk management team adds is a larger vision of cross-departmental priorities, as well as knowledge of how well those non-IT departments are educated and prepared to function when the disaster hits. A DR plan that ensures five nines of uptime and uninterrupted mission-critical system access is going to be a failure if line-of-business managers and staff are physically unsafe or isolated, or unaware of the alternate means of access.

Ideally, the risk management team will be a part of the initial disaster recovery planning process, and will then be well-positioned to assist the IT department with

- Gathering business requirements for the planning process
- Drafting procedures and instructions for all departments and updating these documents at prescribed intervals
- Testing plans and procedures
- Training departmental managers on disaster recovery, who will then train their groups on DR procedures
- Communicating procedural or staffing changes in non-IT departments to the IT group, when those changes create the need for updates to the plan

Backup and Recovery Across Heterogeneous Environments

Arthur Cole, Infrastructure

Backup and recovery systems have never been all that easy to deal with. Not only are they expensive to build and maintain, but they need to accommodate increasingly diverse data center infrastructure that has become both more virtual and more heterogeneous in nature.

B&R, in fact, has a tendency to follow the divergent paths of the data center at large — as new systems are deployed in a not altogether coordinated fashion, their associated recovery components end up creating a hodgepodge of platforms that can be unwieldy, at best, in the frantic rush to get services up and running again.

Naturally, then, disaster recovery across heterogeneous infrastructure is proving to be a hot commodity, as storage and networking firms look to shore up their capabilities in preparation for even more advanced cloud architectures. A company called Unitrends has made several strategic moves to align its Enterprise Backup virtual appliance, which operates across Hyper-V and vSphere deployments, with high-speed data center platforms.
In recent weeks, the firm has teamed up with Nexsan to form an integrated backup system with the E-Series SAN and NST5000 Unified hybrid storage solution, while at the same time joining forces with with ExaGrid, a maker of scalable, disk-based backup systems. In both cases, the overriding goal is to provide for both rapid recovery and broadbased reach into widespread enterprise infrastructure.

This may be well and good for enterprises looking to revamp their entire recovery infrastructure. However, for those that would still like to utilize their existing platforms, there are ways to integrate them into a more cohesive whole. A company called Bocada, for example, provides a backup management and analytics system that drills into disparate systems to ascertain their performance. From a single dashboard, users can analyze individual backup operations, not just servers of virtual machines, and then adjust policies to correct deficiencies and improve on successes.

The reality of heterogeneous environments is also hitting home for the top virtualization players. VMware recently announced that its vFabric Data Director 2.0 will support Oracle databases within the vSphere environment, which should make it easier for developers to create all manner of multi-vendor database applications, including provisioning, cloning and backup. vFabric now supports Oracle 10gR2 and 11gR2, as well as Postgres 9.1, and provides access to various development environments through the GemFire, SQLFire and Spring frameworks.

Heterogeneous environments come into being primarily from the twin drives of increasing operation performance and flexibility and cutting costs. That they tend to follow haphazard development paths has more to do with budgetary constraints than lack of foresight. After all, not many enterprises have the resources to build fully integrated data center environments from scratch.

When it comes to devising a cohesive backup infrastructure for these disparate environments, however, most organizations will keep a close eye on the bottom line in the hopes that overall performance will never truly be tested in real-world situations. Fortunately, with a heterogeneous backup system to match existing data center environments, enterprises will find themselves with the best of both worlds: low costs and a thorough recovery platform.

Preparing the Business for an Active Hurricane Season

Carl Weinschenk, Data and Telecom

A business had no excuse for not being prepared for hurricanes a decade ago. After Hurricane Katrina and Hurricane (and then Superstorm) Sandy, there is even less rationale to not take the necessary steps, especially if the business is located in the area most likely to be pounded. Unfortunately, that area seems to be getting bigger.

Last Saturday was the beginning of hurricane season, and May 26 to June 1 was National Hurricane Preparedness Week. Unlike some crises, such as fires and power outages, hurricanes and other weather-related challenges are vaguely predictable. That's a good thing. The other good news is that a tremendous amount of information is available on hurricane preparedness and, more generally, on business continuity/disaster recovery.

In short, it's impossible to guarantee that hurricanes won't cause disruption or worse. But it is possible to greatly minimize the impact.

For those who have sat on the sidelines, now is a great time to get engaged. The National Oceanic and Atmospheric Administration (NOAA) said in late May that this year's season likely will be an active one:

> For the six-month hurricane season, which begins June 1, NOAA's Atlantic Hurricane Season Outlook says there is a 70 percent likelihood of 13 to 20 named storms (winds of 39 mph or higher), of which 7 to 11 could become hurricanes (winds of 74 mph or higher), including 3 to 6 major hurricanes (Category 3, 4 or 5; winds of 111 mph or higher).

The press release says that the number is "well above" the average of 12 named storms and six hurricanes, half of which are considered major events.

Hurricane preparation literature lends itself to lists. The International Business Times, for instance, suggests understanding the differences between hurricanes and tropical storms and watches and warnings, keeping emergency contact information at hand, having emergency kits ready to go, planning an emergency escape route and staying calm.

There is not too much new to say about hurricane preparation. Much of it is common sense. What is considered smart for families also is appropriate, with tweaks, for businesses. The most important steps are to pay attention and take hurricanes seriously. Indeed, in an era characterized by two intensely destructive storms – Hurricane Katrina preceded Hurricane (and then Superstorm) Sandy by seven years – the rationale for not preparing gets thinner and thinner.

There are differences, compared to a decade ago, in hurricanes, hurricane preparedness and how businesses deal with the storms. On the positive side, folks generally are more aware and the trends in telecommunications – cloud-based networks, mobility and increasing work-at-home time – tend to lessen the disruption. The downside, however, is that storms seem to be getting worse.