Acronis

The **7** Rules of **IT Business Continuity**

How to protect your company, your customers and yourself with IT BCDR

The concept of IT Business Continuity and Disaster Recovery (BCDR) has been established for quite a while, however actual implementation varies across solutions, vendors and industries. It may look easy on the surface: plan, backup, replicate and test. Sounds simple, right? Not so fast. The devil, as they say, is in the details. Let us take a look.

> “
>
> **80% of organizations** aiming for higher levels of operational maturity will fail without proper implementation of BCDR management planning tools.[1]
>
> ”
>
> - **Gartner**

30,000-FOOT VIEW

First let’s understand the goals of BCDR. The key drivers for BCDR are:

1. Surviving unplanned events

Many kinds of events can cause interruption or degradation of IT service: natural disasters, technology failures, user errors, etc. While natural disasters, terrorist acts, or malicious data breaches certainly are more known, operational events — not disasters — are the leading cause of IT outages. According to Forrester Research[2], simple loss of power is still the leading cause of downtime, closely followed by IT hardware, software, and network failures. It’s important to understand the difference in consequences: while natural disasters and fires can potentially take an entire site out of commission for significant time, technical failures or HR issues are usually localized and can be resolved quickly.

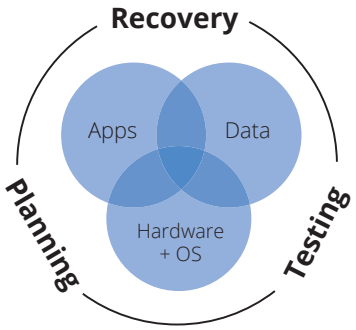
> “
>
> It’s still mundane events such as **power failures, IT failures, and human error** that top the list of causes.[2]
>
> ”
>
> - **Forrester**

2. Assuring IT continuity through regular operations

Beyond unplanned IT outages, modern BCDR is increasingly driven by the need for much higher IT service stability and agility. Planned operational procedures like software and hardware upgrades, facilities maintenance, and data center migrations, as well as organizational changes and M&A activities, require IT to be highly adaptive and agnostic of its physical infrastructure and location. IT service continuity is a critical requirement, so organizations are looking at BCDR as the means to assure IT’s continuous operation through any kind of planned operational events.

THE UNDERLYING TECHNOLOGY

Whatever the underlying technology, disaster recovery (DR) solutions must restore three key components:



1. Data
2. Infrastructure (hardware and OS)
3. Applications

Data backup creates additional copies of data — files and folders — on- or off-site. Data backup technologies have been developed over the years to minimize backup storage size (deduplication), lower network traffic loads (compression), ensure the security of the data in transmission and at rest (encryption), and ultimately shorten the backup window. All of these improvements have optimized data backup over time, bringing it to the point where typical backups can be considered a commodity in IT datacenter operations.

Systems replication creates a secondary copy of the critical IT environment: servers, databases and networks, both physical and virtual. When the primary data center is unavailable, the replica can be started and used until the original environment is available. There are few kinds of architectures and relationships between the primary and the replica data center, depending on how critical the environment is, the availability of
facilities for the secondary data center, and budget. With the proliferation of cloud-based services, it is becoming increasingly common to use multi-tenant cloud disaster recovery services offered by the leading DR vendors, or a hybrid combination of on- and off-premise services.

> “Because server and data restoration on demand do not require the preallocation of specific computing equipment or floor space, customers have the opportunity to exercise their recovery plans frequently.[3]”
>
> - **Gartner**

VIRTUALIZATION CHANGES IT ALL

In a physical server environment, multiple point solutions can individually provide data backup and systems replication. However, due to the increasing virtualization of IT environments and the growing popularity of software-based infrastructure (data, networks), all of these components can be protected as a single virtual machine environment. Virtualization highly simplifies disaster recovery solutions, reduces costs, and provides stronger assurances of achieving the promised recovery point objective/ recovery time objective (RPO/RTO) based on clearly defined SLAs.

> “As traditional approaches to DR become outdated and less effective, DRaaS providers with tunable resiliency levels, broad platform support, and favorable contract terms and pricing will lead the pack.[5]”
>
> - **The Forrester Wave** ™

THE DEVIL IS IN THE DETAILS

BCDR can be implemented in many forms, delivering different levels of protection at varying costs. It could require a significant investment — in an environment of shrinking IT budgets and HR resources. Calculating the ROI of BCDR is beyond the scope of this paper (see The ROI of Disaster Recovery white paper for more information), but it is critical to ensure the success of the BCDR solution designed to protect your IT service.

We have identified several best practices to keep in mind when architecting your BCDR solution:

1. Plan ahead and document

Well-documented action plans in cases of planned or unplanned service interruption must be available so your IT personnel can respond efficiently. The plans should include detailed recovery procedures and BCDR vendor engagement rules, as well as means of communication and transportation options. When do you declare a disaster? Where are the copies of data, software and licenses stored? What's the acceptable data loss, and how fast do you need to recover? At a minimum, detailed plans must be available in paper/hard-copy form, but it's much better if they are also accessible to your distributed staff in digital form.

2. Replicate applications

Data backup is fundamental to BCDR, but, by itself, it cannot ensure continuity of your operations. Without functioning servers, data is useless. Rebuilding hardware/software and loading the data can take a while. Having a secondary site with all applications and data replicated is one possible solution, but it may not be financially viable for small to midsize businesses. With the power of the cloud, disaster recovery can be offered as a service (Disaster Recovery as a Service, or DRaaS), based on multi-tenant remote replication. Leading vendors can guarantee SLA-based availability of your applications and data out of DRaaS data centers through a secure Internet connection. Your restored IT service can be available within the promised timeframe — often as little as 15 minutes — until your primary site is back online.

> One in three companies has declared a disaster during the past five years.[2]
>
> - **Forrester**

> Cloud-based backup and disaster recovery solutions are the #1 cloud service that IT is planning to start using within the next 6 months, across all geographies and company sizes.[4]
>
> - **SpiceWorks**

> Cloud-based recovery services have evolved from traditional, managed disaster recovery (DR) services adopted by enterprises and online backup services adopted by small or midsize businesses.[3]
>
> - **Gartner**

3. Establish on- and off-site protection

Modern BCDR technology offers both on-site and remote protection. Each option has its advantages. Protecting locally allows easier access to your data and a generally faster recovery rate. Local replication, however, only works when your primary environment is still accessible. In cases of major disaster or for long-term data retention, you need to protect your data and applications off-site, preferably in a geographically distant location that will be unaffected by any local event. Today, best-of-breed BCDR technologies offer hybrid solutions that give you the best of both worlds: an on-site appliance for fast access, plus efficient replication of your environment in the cloud for ultimate protection.

4. Automate recovery procedures

Your IT staff may be the best in the world, but in case of disaster you may not want to rely on their flawless execution of complex processes; the probability of human error is especially high under the pressure and uncertainty of a disaster. Imagine your personnel manually starting multiple servers, recovering and validating data, testing network connectivity and executing many other critical tasks when every mistake can cause lost data or prolonged service outage — and them weighing it against the safety of their families. In addition, your key personnel may not even be available as they take care of their own families. This is why a "push of a button," process-driven disaster recovery approach offers higher ROI, especially in environments with limited IT resources and expertise. Modern BCDR automation includes conditional dependency tests, parallel threads, manual work flows with notifications, and other elements that make your recovery reliable, repeatable and testable.

> "Automate, automate, automate. The complexity of today's technology is beyond what humans can manage."[2]
>
> - **Forrester**

5. Test regularly

Experience tells us: test well, test often. A disaster recovery solution is only worth the cost if you know that it will actually work; otherwise it is a wasted investment. Even if your plan was perfectly designed and tested on deployment, your environment will change over time. Hardware and software upgrades, network tweaks, personnel training and turnover issues can all affect the success of your BCDR procedures, even in a fully automated environment. That is why it is so important to test your DR plans — as often as logically feasible. Advanced BCDR solutions provide built-in testing facilities, a separate virtual network for testing, and test scheduling.

> "With DRaaS, testing is generally automated and nondisruptive, which means you can test more often."[5]
>
> - **The Forrester Wave** ™

6. Secure your backed-up environment

Security is always a concern, and BCDR is not an exception. For locally-hosted BCDR solutions, the security is the same as what you've already established for your primary data and applications. Trusting the cloud with your BCDR needs, however, has its challenges. Especially for highly-regulated industries, keeping data in the cloud private and secure is a major requirement. Many standards and directives require that organizations protect their data and provide defenses against threats. Ultimately, the data centers used by the DRaaS providers must demonstrate the highest levels of security by themselves. Additionally, a data encryption option should be available to protect data locally, in transmission, and at rest in remote storage facilities, with the proper key management and administration.

7. Select your BCDR partner wisely

It is important to stick to someone who understands, and has a deep installed base in your industry. That way you know your questions and issues will not be new to them, and will not require a lot of research in the midst of a situation requiring quick response. Proven and independently validated superior technology and thought leadership can help you avoid doing an extensive research and vendor verification on your own. There is a plethora of IT industry analysts covering the BCDR space — check with them before you make your choice.

NEXT STEP

To summarize, BCDR is your IT insurance policy and the protection mechanism mitigating your risks. We have outlined key points of consideration to ensure your BCDR solution will work when you need it most, and given an overview of the available options. It is better not to do it yourself — work with a professional who has done it before.

Resources

1. Gartner: Predicts 2014: Business Continuity Management and IT Disaster Recovery Management, by Roberta J. Witty, John P. Morency, Dave Russell.
2. Forrester: The State of Business Technology Resiliency, Q2 2014, by Stephanie Balaouras.
3. Gartner: Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2014, by John P. Morency, Roberta J. Witty.
4. Spiceworks Annual State of IT report, 2014.
5. The Forrester Wave™: Disaster-Recovery-as-a-Service Providers, Q1 2014, by Rachel A Dines

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment - virtual, physical, cloud and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com** / Follow Acronis on Twitter: **http://twitter.com/acronis**