Acronis

WHITE PAPER

The 7 Rules of IT Business Continuity

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

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

The concept of IT Business Continuity and Disaster Recovery (BCDR) is not new; 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's take a look.

30,000-FOOT VIEW

First, let's understand the goals of BCDR. The key drivers are:

1. **Surviving unplanned events**
   Many kinds of events can cause interruption or degradation of IT service: natural disaster, 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, a simple loss of power is still the leading cause of downtime, closely followed by IT hardware, software, and network failures.2 It's important to understand the difference in consequences. While natural disasters and fires can potentially take an entire site out of commission for a significant time, technical failures or HR issues are usually localized and solved quickly.

2. **Assuring IT continuity through regular operations**
   Beyond unplanned IT outages, the need for much higher IT service stability and agility drives modern BCDR. 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 unplanned operational events.

"Consider that a risk reported in the global news cycle doesn't automatically make that a risk for every organization."[1]

"It's still mundane events such as power failures, IT failures, and human error that top the list of causes."[2]

THE UNDERLYING TECHNOLOGY

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

Data
Infrastructure (hardware and OS)
Applications

Data backup creates additional copies of data – files and folders – on-premises 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. These improvements have optimized data backup over time, bringing it to the point where typical backups can be considered a commodity in IT data center 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-premises services.

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 (RPO) and recovery time objective (RTO) based on clearly defined SLAs.

"Backup is an action, while BCDR is more of a formula based on a sequence of actions that address protection of all or part of a business IT environment...It is all about data you could lose. Without data, you have nothing."[3]

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, BCDR vendor engagement rules, and 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 or hard copy form, but it's much better if they are also accessible to your distributed staff in digital format.

2 Replicate applications

Data backup is fundamental to BCDR, but by itself cannot ensure continuity of your operations. Without functioning servers, data is useless. Rebuilding hardware or 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 the SLA-based availability of your applications and data from 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.

"As the rapid rate of business changes force changes in IT, it is critical for companies to update their plans continuously. This is something only 10% of organizations do today."[2]

"In the near future, many IT departments will be tasked with addressing new security concerns, enabling more seamless communications between physically distant coworkers, migrating workloads to the cloud – 27% plan to refine disaster recovery plans to account for additional scenarios."[4]

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 disasters 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 that against the safety of their families. In addition, your key personnel may not even be available as they take care of their own families. A "flip-of-a-switch," 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 workflows with notifications, and other elements that make your recovery reliable, repeatable, and testable.

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.

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

"Without the testing and verification of DR plans, you'll have no idea as to whether or not you'll be able to recover from a disaster or extended outage. It's during these testing periods that any security and backup issues can be identified and addressed because sometimes, extended downtime can be a life-or-death situation."[5]

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

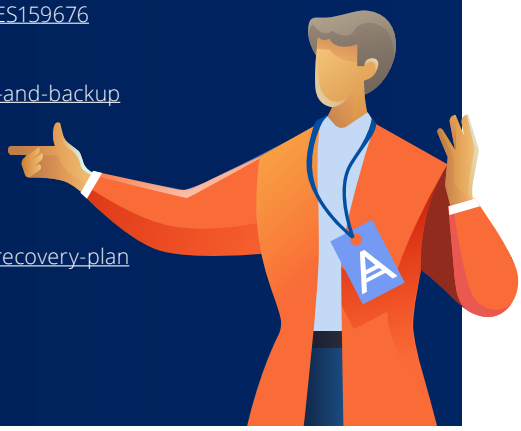
It is essential to stick to someone who understands and has a deep installed base in your industry. That way, you know your questions and issues will not be new to them and will not require a lot of research in a situation requiring a quick response. Proven and independently validated superior technology and thought leadership could help you avoid doing extensive research and vendor verification on your own. There are many 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. Stress-Test Your Business Continuity Management, Smarter with Gartner, Gartner, February 2020. www.gartner.com/smarterwithgartner/stress-test-your-business-continuity-management/
2. The State of Business Technology Resiliency 2020, Forrester, August 2020. www.forrester.com/report/The+State+Of+Disaster+Recovery+Preparedness+In+2020/-/E-RES159676
3. Don't cut corners with disaster recovery and backup, TechTarget, March 2020. https://searchdisasterrecovery.techtarget.com/tip/Dont-cut-corners-with-disaster-recovery-and-backup
4. Annual state of IT, Spiceworks, 2020. www.spiceworks.com/marketing/state-of-it/
5. How often should you test your disaster recovery plan?, ConnectWise, January 2019. www.connectwise.com/blog/business-continuity/how-often-should-you-test-your-disaster-recovery-plan



Acronis

Learn more at
www.acronis.com