Disaster Recovery in the Cloud Era

By Frank Ohlhorst

APRIL 2018 | US$25 | S060418

Channel Partners™

Channel Futures™

Disaster Recovery in the Cloud Era

By Frank Ohlhorst

APRIL 2018 | US$25 | S060418

Channel Partners™
Channel Futures™

Table of Contents

Channel Partners™

About the Author

linkedin.com/in/fohlhorst
@fjo_writes_tech

FRANK J. OHLHORST is an award-winning technology journalist and technology analyst, with extensive experience as an IT business consultant, editor, author, presenter and blogger. He frequently advises and mentors technology startups and established technology ventures, helping them create channel programs, launch products, validate product quality, design support systems and build marketing materials, as well as create case studies and white papers. Ohlhorst also provides forensic services for data security, assists with compliance audits and researches the implications of compliance on a given business model. Ohlhorst has held the roles of CRN Test Center director, eWeek's executive editor and technology editor for Channel Insider, and is an editor-at-large for Channel Partners and Channel Futures.

Disaster Recovery in the Cloud Era

BUSINESS CONTINUITY AND DISASTER RECOVERY GO HAND IN HAND TO ENSURE RESILIENCY IN THE MODERN

enterprise. However, the requirements and objectives of BC/DR vary from customer to customer, and the two sides of the coin don't always align.

Business continuity plans focus on keeping systems up and running *in spite* of outages using failover, replication and other technologies. However, effective business continuity can be expensive and may not hold up in the face of serious disasters, such as loss of a facility or a massive malware or DDoS attack that brings business to a halt. Many customers implement business continuity only for mission-critical applications, such as e-commerce, databases and accounting systems.

Disaster recovery services should be sold as a fail-safe, a set of processes, technologies and policies to restore systems to operation in case of a disaster that overwhelms the business. Simply put, disaster recovery should kick in when business continuity fails.

That said, disaster recovery solutions face some of the same constraints and guidelines as business continuity systems. For example, disaster recovery plans generally prioritize the recovery process based on the importance of the systems protected. That means line-of-business and revenue-generating applications are the first restored to functionality, while other less-critical processes are placed on the back burner.

Decisions as to what is mission-critical, how much to spend, the right RTO and RPO metrics and whose apps go on that back burner can be minefields — no line-of-business

leader wants to hear that his or her systems are expendable. An impartial, trusted adviser can help with this effort, but still, DR is complicated to implement and may have many moving parts that can be difficult to manage, as well as validate.

DRaaS simplifies things, as we'll discuss, but cloud services don't negate the core challenge: How can customers rely on their DR plans if all possible scenarios are not thought out, critical systems are not identified and they don't see proof of recoverability?

Short answer, they can't.

DR By The Numbers

The statistics are sobering and illustrate how important properly configured and validated DR solutions are:

- **20 percent** of businesses experience a failure — fire, flood, power outage, natural disaster — in any given year, and 80 percent of those businesses will go under in just over a year. *—Bureau of Labor*
- Only **35 percent** of SMBs have a comprehensive disaster recovery plan in place. –Gartner
- Unplanned downtime costs companies between **$926 and $17,244 per minute**. *—StorageCraft*
- Seven out of every 10 malware payloads were ransomware. Just ask the City of Atlanta. *—Malwarebytes*

Big Picture Plan

Whether systems reside in the cloud, on premises or a mix, effective DR starts with a plan. Countless books have been written on what a disaster recovery plan should cover, but some central themes break down into five high-level best practices:

Establish communications rosters and role assignments: A plan for reaching all primary IT stakeholders, service providers, cloud and connectivity suppliers and employees is essential. Make sure this document isn't stored on a server that may now be infected with ransomware or in a binder that could be under water. Partners should keep multiple versions of full contact information for each customer, along with appropriate roles so all participants know what is expected of them in a disaster.

Create a detailed asset inventory: Knowing what systems must be protected and which applications are critical, and being able to prioritize the importance of systems to business operations, is key for building a plan that promotes recovery in an efficient and logical fashion.

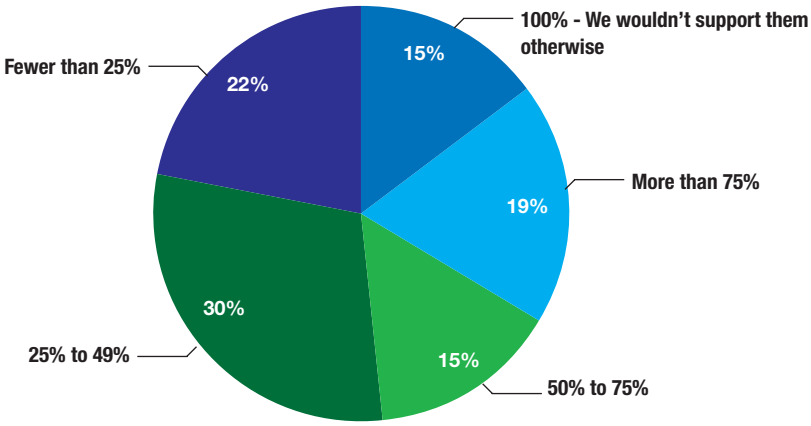
Implement backup and recovery technologies: Knowing *what* to protect is only one part of the process; determining *how* to recover those assets is the most critical step in defining a DR plan. Selecting the technologies to protect hybrid systems can be a complex endeavor. Partners need to consider factors including customer storage requirements, offsite backup capabilities, the need to restore applications and data to dissimilar systems, and so forth.

Treat the plan as a living document: Any changes in infrastructure, applications, locations, policies, cloud providers and so forth should be recorded and addressed in the disaster recovery plan. Conduct regular audits to make sure all critical customer systems remain protected and included in the scope of the plan. For partners, this is a great high-touch consultative opportunity.

Testing and validation: Businesses need to regularly test their disaster recovery plans. That means simulating a disaster and making sure the organization can recover from it, within the parameters outlined in the plan. Testing not only validates the plan, it can also uncover glitches in the system, show where policy changes may be needed and give a better indication of TTR (Time To Recovery).

These five steps comprise a road map. However, thanks to cloud technologies, the world of DR is undergoing change, and customers may have to realign existing DR plans and solutions to address how the cloud changes the technological landscape.

What percentage of your customers have effective business continuity/disaster recovery (BC/DR) plans?



* Figures do not total 100% due to rounding
Source: Channel Partners BC/DR Survey, 2017

DR and the Public Cloud

The introduction of cloud services brings new and interesting twists into the DR equation — it's a calculation that can either become more complex due to the cloud or greatly simplified. A lot depends on whether customers get good advice from their advisers.

Say a customer's cloud portfolio includes the typical productivity and business SaaS and IaaS, along with platforms, storage, security and a few other functions delivered in an as-a-service model. Each has an impact on how disaster recovery is handled.

For example, when businesses use a SaaS product, such as Salesforce, the applications and data are stored within the Salesforce cloud, which shifts the burden of business continuity and DR to Salesforce. Of course, partners should still establish a method for backing up customer data with a third-party solution like Druva, Veeam or Veritas.

What are the most significant drivers for investing in a BC/DR strategy? Please rank in order of importance.
1 Security: Ransomware, malware or other threat
2 Connectivity failure
3 Equipment failure
4 Future possible natural disaster
5 Insistence by line-of-business leaders
6 Previously burned by disaster, data loss or other externally driven failure
7 Power failure
8 Other

Source: Channel Partners BC/DR Survey, 2017

Businesses choosing IaaS and PaaS may encounter a similar situation, one that redirects how DR is implemented and managed. With IaaS, compute resources, networking and storage are moved into the cloud, potentially offering more reliable hardware and integrated business continuity. That said, IaaS adopters must still install applications, configure virtual systems, define networking and perform many of the same chores that would be accomplished on in-house infrastructure, including security and patching. It's called "shared responsibility," and it's an important message for partners to convey to customers who think shifting a service to AWS or Azure takes away the need to monitor settings and protect applications, data and other resources.

In particular, you still need to backup data stored in the cloud because catastrophes can happen even to large CSPs. They can take the form of corrupted databases, ransomware attacks, faulty patches, even the cloud provider going dark because of human error, power outages or a DDoS attack. Much the same can be said for PaaS, which is susceptible to the same types of disasters that potentially plague IaaS.

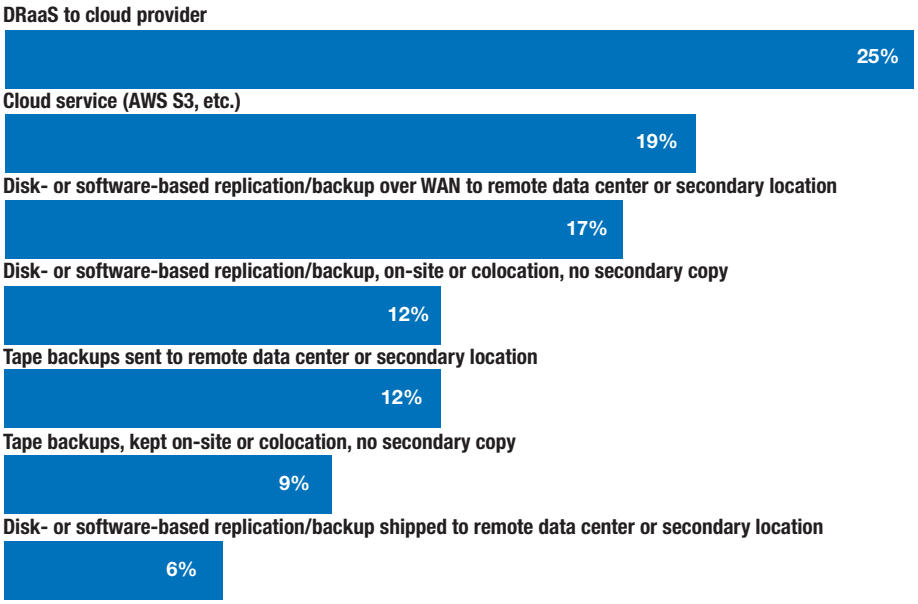
Bottom line, help customers understand what's in the fine print, know what SLAs they're paying for and outline options to keep the business running if a cloud provider suffers extended downtime.

Digital Transformation, DR and the Cloud

Many customers are in the thick of digital transformation projects, where legacy processes are being digitized and moved into the cloud. Digital transformation also entails using digital advances, such as analytics, mobility, social media and smart embedded devices, as well as improving the use of traditional technologies, such as ERP, to improve customer relationships, internal processes and value propositions.

Simply put, digital transformation can be a disruptive process with far-reaching implications for disaster recovery. As legacy or manual systems are moved into the digital realm, they must remain protected.

What backup components are included in customers' BC/DR plans? Select all that apply.



Source: Channel Partners BC/DR Survey, 2017

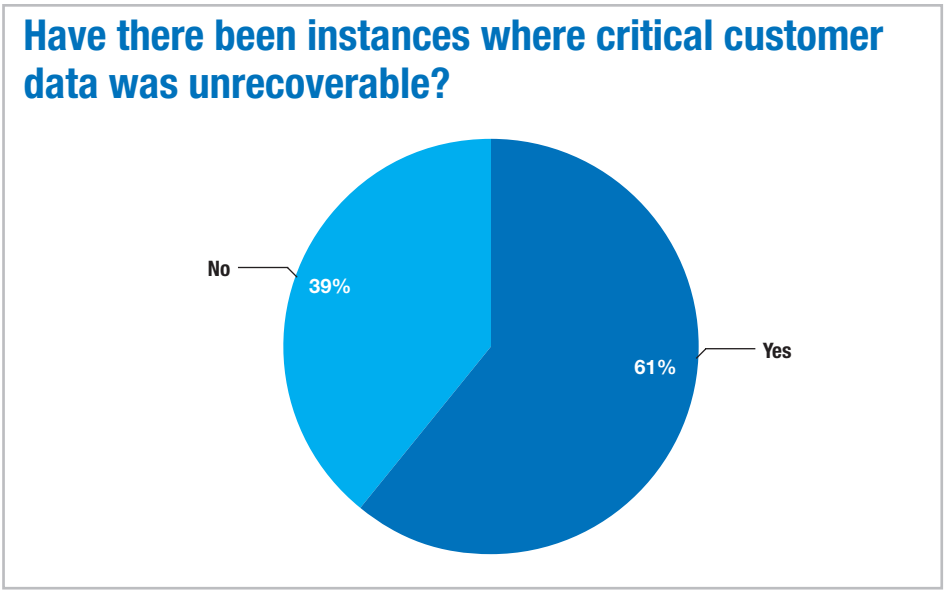
What's more, digital transformation can introduce different compute models, including as hybrid clouds, private clouds and IoT devices, all of which, again, bring additional complexity to DR. Helping customers solve for those challenges requires an understanding of what processes are being digitized, how important those processes are to the day-to-day operations of the business, and how long the business could do without.

For partners managing DR, institute new methods of validation as digitization progresses. For example, new applications may be housed in a hybrid cloud, where some resources are on premises and others are on a public cloud. To fully protect those workloads, administrators must understand how those applications interact with back-end resources, where data is stored and what integrations are necessary for those applications to function.

Digital transformation may also introduce the concept of APIs, where small pieces of predefined code are used to allow applications to interact with other resources, which can be internal or external. APIs may be persistent or non-persistent, used regularly or occasionally. Nevertheless, these integrations may be a critical part of the application, even if that API supports only a quarterly or monthly process.

Hybrid cloud applications using APIs for cross-platform integrations can be especially difficult to test under a simulated failure, meaning that DR testing may not be comprehensive enough to guarantee full recovery during an actual disaster.

These concerns and many others have driven many administrators to shift DR into the cloud itself. Partners are well aware the prevalence of DRaaS (disaster recovery-as-a-service) solutions, which shift all the elements of DR into the cloud. In our recent Channel Partners survey, 78 percent of partner respondents said they currently sell DRaaS. Top channel-focused providers include Carbonite, Datto, Zerto and Veeam.



Source: Channel Partners BC/DR Survey, 2017

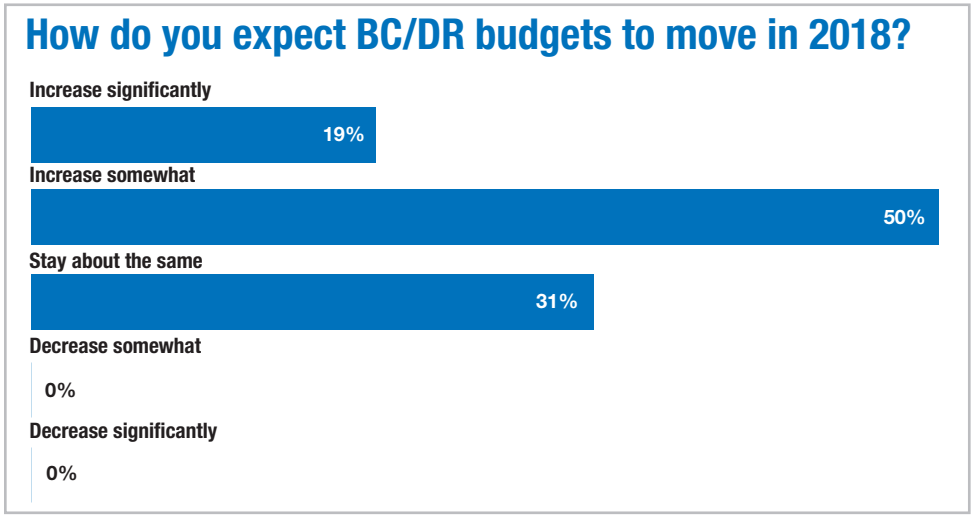
While it's true DRaaS has the potential to greatly simplify the recovery process, when advising customers, make sure you're up-to-date on the SLAs offered by various providers to make sure recovery is guaranteed within what the business considers a reasonable amount of time. Ensure the service provider enables the IT team or your staff to do frequent recovery tests, and that audits and other due diligence chores are up-to-date. Those processes should also be verified independently.

The Importance of Cloud Recovery Testing

Regardless of the type of disaster recovery solution a customer selects, regular testing is indispensable. Never assume that a DR product — cloud or not — works as advertised and is configured correctly for the customer. Thorough testing is a must; most experts recommend at least quarterly. Almost no one does so. In our BC/DR survey, 61 percent of channel pro respondents said there have been instances where critical customer data was unrecoverable.

There are reasons companies shy away from testing. For example, it may be difficult to take down an active cloud instance to perform a test. Not all businesses have the capability to simulate an actual disaster and shutdown active systems. However, that doesn't preclude testing the restore process. In most cases, it is still possible to perform cloud recovery testing that simulates a real recovery following a major catastrophe. That testing can be accomplished by using an isolated network segment, so the production network is not visible to the recovery process. That way, the recovery testing does not in any way interfere with the production network, and the test also validates the ability to move production systems into an alternate environment.

These tests have several real-world goals, including proving you actually can recover data after a disaster, determining what it takes to recover from a disaster, benchmarking the recovery process, validating bandwidth capabilities and determining the performance of the DRaaS system being used. Testing may also uncover other

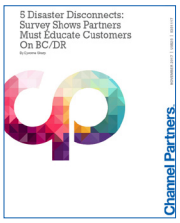


Source: Channel Partners BC/DR Survey, 2017

concerns that can be addressed before a real disaster happens. Potential issues include validating digital certificates and garnering a better understanding of controls, management consoles and progress indicators. What's more, testing should allow administrators to explore various recovery types, such as partial restores, retrieval of archive data, bare metal recoveries and so forth. Other elements that can be checked include infrastructure issues, such as DNS servers, DHCP servers, directory services, file and folder shares, and so on.

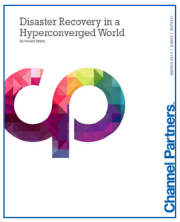
Testing should be documented. Even with DRaaS, customers should have run books, where expectations and test results are clearly laid out. Documentation will provide those performing a recovery with invaluable insights, lessons learned and guidelines to accomplish recovery as quickly as possible.

Related Reports



5 Disaster Disconnects: Survey Shows That Partners Must Educate Customers on BC/DR

We surveyed channel partners and IT pros about the state of business continuity and disaster recovery strategies, and the results show a definite need for channel partners to deliver education on the realities of BC/DR preparedness. Bottom line: Despite what customers think, it not only can happen to their businesses, it probably will.



Disaster Recovery in a Hyperconverged World

Hyperconvergence simplifies IT infrastructure design by integrating the storage layer with compute and networking. This reduces complexity and saves money, but it also requires changes in how customer data and applications are protected. This Report explains how to think about disaster recovery solution in the context of HCI.

DR in the Ransomware Age: Isolated Recovery, DRaaS andEmbracing IT Resiliency

Ransomware attacks are becoming more frequent, complex and sophisticated. Security experts agree, it's not if an attack will come, but when. Disaster recovery can be your customers' best line of defense. This Report explains how the right tools can help you arm yourself against the devastating effects of ransomware.

UC Demands Rethinking Disaster Recovery Plans

Voice and UC in the cloud have created expectations of 24/7 contact among your clients and their customers. Helping this happen requires good planning and system design — and represents professional service opportunities for partners. This report examines what's involved in communications disaster planning, as well as the professional services opportunities it presents to partners.