Summary Insights: DR/BC in a Hybrid Multi-Cloud WFH World

RFG Perspective: The good news – and bad news – is that disaster recovery/business continuity (DR/BC) options have expanded tremendously with the advent of the cloud. In today's New Normal business world, the customary maxims about DR/BC still apply: organizations should design for failure – and they should standardize their DR/BC best practices and simplify. These principles also apply to workloads that have migrated to the hybrid cloud. And, surprisingly, they extend to how one works with SaaS providers as well, who may – or may not – provide automatic data backup. Business and IT executives should ensure that all applications and datasets are implemented with these axioms in mind – the survival of the enterprise could depend upon it.

Virtually all organizations have outages, with the average outage lasting almost two hours. In the new hybrid multi-cloud environment, data and applications are now spread across data centers (DCs), private clouds, public clouds and SaaS providers with data scattered (globally, in some cases) across many types of databases, file shares, and shared storage. That variety speaks to a company's history of data storage – but it also betrays a vulnerability to inadequate DR/BC capabilities.

Lost and vulnerable data caused by an outage damages an organization's brand and its relationships with customers – and sometimes these outages make the news headlines.

Executives and customers expect IT will keep their applications and data running, available, recoverable and safe at all times. That is why the shift to the Cloud and Edge environments must ensure that RTO/RPO (recovery time objective/recovery point objective) requirements cannot be relaxed.

In this RFG100 video conference, customers discussed the challenges and best practices for BC/DR in their computing environments – which now span customers' core data centers, hybrid clouds, and the Edge (e.g., factories, stores, remote locations). The central topic: how to ensure that data dispersed among many locations is current – and "clean" – for end-user access, data analytics, and effective business use.

The RFG100 Panel's Key Takeaways on Data Cleansing Options

On Oct. 14, 2020, RFG facilitated a videoconference on "DR/BC in a Hybrid Multi-Cloud WFH Environment." The panelists on the call were:

- Mick Kaleci, Managing Director, Deloitte
- Frank Breedijk, CISO, Schuberg Philis
- Mike Mitsch, Director, NEC America
- Jean S. Bozman, President, Cloud Architects llc

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

A real-time poll of the RFG100 attendees revealed several key takeaways:

- 40% of respondents test their disaster recovery (DR) procedures annually; while 30% test DR quarterly and 30% test DR monthly
- More than 45% of respondents said they had human-readable data dictionaries; only half that amount said they had machine-readable data.
- 70% of respondents have not changed the frequency of their planned DR tests since the COVID-19 crisis began.
- 70% of the DR tests were done internally by IT staff. Fully 80% of respondents said they use the cloud for part of their DR procedures, while only 10% reported using any disaster recovery as a service (DRaaS) provider.

RFG Analysis

When the COVID-19 crisis began, organizations launched work-from-home (WFH) policies that quickly shifted their employees out of the office—and into a variety of at-home work environments.

Rapid extension of VPN network links to the home supported WFH in just a matter of weeks this spring. Many companies leveraged virtual desktop interface (VDI) technology to protect mission-critical applications being accessed from home. Now, many organizations are re-examining their DR/BC procedures for this new WFH environment, and the best practices protecting applications that are being accessed by out-of-office employees over extended periods of time.

Standardize and Simplify

The rush to WFH, Cloud and Edge in some cases has created additional DR/BC challenges, because existing DR/BC practices were adopted with minimal changes for WFH, Cloud and Edge solutions. This approach to DR/BC could drive up operational costs (OpEx) and cause unexpected failures. We believe that now is the time for executives to re-examine their processes for standardizing and simplifying their DR/BC practices globally. Areas to be examined are:

- Seamless connectivity and availability for end-users
- Redundancy
- Split tunneling (of corporate networks) and load balancing
- Golden images for device hardware and software standardization and preconfigured systems
- Plug-and-play for data centers
- Standardization and licensing

Secure Business Continuity

Work from Home (WFH) employees need seamless connectivity, supported by virtual private network (VPN) and virtual desktop (VDI) technologies. These two forces render home the "virtual" equivalent of being in an office. But to achieve the equivalent of the standard office environment, connectivity must be supplemented with an acceptable level of availability, DR/BC, performance, privacy, and security.

Enterprises require continuous user availability if they expect to support adequate levels of employee productivity and customer access. One of the panelists stated that he was using overnight deliveries of laptops as part of his break/fix process so that employees would experience minimal downtime due to device failures.

For the data center environment, an availability/upgrade best practice for creating golden images for configurations, supplemented by delivery of preconfigured systems from suppliers, was suggested. While global enterprises may not be able to utilize golden images everywhere, RFG executives posited that the 80/20 rule would be a pragmatic solution for many organizations.

Additionally, if vendors are delivering preconfigured systems and automation tools are utilized wherever possible, then onsite installs could become mostly plug-and-play efforts: That would limit the amount of time and personnel that would otherwise be required to install all of the systems and to put them into production. For added the safety of IT staffers, onsite IT teams should be tested for COVID-19 and only those that test "negative" be allowed in the facility.

IT executives should keep in mind that business continuity is a business issue first and foremost – rather than viewing it as a technology problem. For example, enterprises could use a content delivery network (CDN) provider like Akamai and Cloudflare) to satisfy application availability and latency challenges. Given the option to work with CDNs for help with DR/BC, IT organizations should not be struggling to solve BC problems on their own. Rather, they should be partnering with their corporate and line of business (LoB) executive peers to resolve BC processes and procedures.

Design for Failure

The RFG100 panel suggested that organizations should not focus only on preventing outages. There are infinite ways to fail and the Law of Diminishing Returns prove that worrying about preventing a broad spectrum of causes for outages is not worth the cost. Instead, companies should design with the prospect of failure in mind – while preparing for a quick recovery from failure (outages). Simplification and

Standardization are two key design principles for DR/BC in the WFH world. These principles apply to all aspects of delivering IT services to users and customers – including a close review of their firewalls, networks, routers, servers, storage, and universal power supplies (UPS systems).

The growing use of cloud services for scaling up enterprise applications and database capacity should help IT planners to avoid over-provisioning their organization's on-premises hardware and software. Cloud services have the value proposition of supporting bursting demands for compute and storage capacity – while avoiding on-premises build-out of data centers.

One RFG100 panelist suggested the Netflix Chaos Monkey as a useful approach for constantly testing for failures. The Chaos Monkey software randomly terminates instances in production to ensure that software engineers implement their IT services to be resilient to instance failures. Other RFG100 panelists recommended pro-active testing to detect failures, such as monitoring the IP pool every 15 minutes to check for incidents.

The Utility of Active/Active Operations for Non-Disruptive Failovers

As for data center protection, a number of RFG100 panelists cited the need for active/active links with load balancers and VLANs (virtual LANs) to back-up the data from compute and storage resources and provide instantaneous failover. While active/active operations have long been the gold standard for back-office workloads, organizations must now take stock of where that same standard should be applied to distributed applications – running across hybrid clouds – and distributed data supporting those applications.

With the use of Cloud and Edge environments, organizations have the opportunity to implement DR/BC using active/active systems. Moreover, if patch management is included in the mix, then enterprises can actually simplify some of their processes while simultaneously reducing their chances of failures. For overall simplicity in cloud environments, DR for a given workload should be done within the same CSP, using multiple availability zones and regions to ensure redundancy for DR/BC.

Here's how proactive patching and updating works: customers can make one of the active/active systems "non-active" and then apply the patches to the appropriate software without creating an outage to end-users. RFG100 panelists said this behind-the-scenes patching process could be done monthly, weekly, or more frequently, if needed. Its advantages include keeping software current, making failovers more predictable, and reducing the frequency of outages caused by failovers and fallbacks.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

Data Privacy Considerations

RFG notes that there are GDPR limitations to be considered, as described in another section of this document that addresses data privacy. Personally identifiable information (PII) data must be copied and protected, in compliance with governmental regulations that vary across the world – by country and by region.

RFG100 panelists observed that there was limited value of executing an application on more than one CSP. That is to say, leveraging a multi-cloud approach is valuable but one needs to recognize that each application has an affinity to a particular cloud or data center environment. With this method, RTO/RPO can be set to zero to achieve continuous availability.

If enterprise data is deployed to the cloud, IT organizations will be able to backup and restore mission-critical data using storage resources and software supported by CSPs (e.g., Amazon's AWS S3, Microsoft Azure's cloud storage, or cloud storage from IBM Cloud or Oracle Cloud). We note here the common customer complaint that data egress charges (removing data from the public cloud – and returning it to the private cloud or the data center) can be very expensive. That's why IT organizations must choose carefully when migrating enterprise data to public cloud services.

Potential SaaS exposures

Guaranteeing DR/BC with one's SaaS providers can be challenging, to say the least. In many cases, the contracts absolve the SaaS provider of any extended outage caused by something beyond its control – the *Force Majeure* clause. When signing up for SaaS – the most widely used category of cloud services, according to IDC global data – IT executives need to fully understand the SaaS provider's DR/BC and data commitments, rights agreements and billing policies.

Customers should not assume that the company's Legal and Procurement departments addressed it properly and that the enterprise is covered and protected by SaaS vendors' data-backup plans. Rather, the firm must find a way to standardize the DR process across all of its SaaS providers.

In July 2020, Salesforce announced that it had stopped backing up customer data – and that it had referred customers to third-party vendors for backup/recovery services. Given that Salesforce is the largest SaaS provider worldwide, there is concern that its decision could prompt a trend for other SaaS providers to cease taking full responsibility for their applications and associated datasets. If this new business model were to become widely adopted by other SaaS providers, it could have a huge impact on IT organizations and their use of SaaS services.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com

Compliance with Data Privacy Regulations

Government regulations require that data policies be consistent across the enterprise (not just a business unit) as relates to what gets stored and when data is deleted or destroyed. For this reason, IT executives must ensure that their cloud providers comply with these regulations, because this is not a data-center issue; rather, it is a corporate policy requirement.

International standards to protect personal information (PII) – notably GDPR in Europe and CCPA in California – must be taken into account. DR procedures must address the chain of custody for key data-stores, ensure data protection for data privacy, and ensure safe access to data stored across the organization.

The increasing reliance on partnerships with cloud providers (e.g., Amazon AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, Oracle Cloud, and others) is having a direct impact on the entire DR/BC discussion.

The good news here is that the cloud providers use sophisticated AI to generate metadata across multiple data-stores – and that they can ensure data replication across availability zones (AZs) in specific geographies. It should be noted that most CSPs charge for inter-AZ and inter-region data transfers so how one chooses to do DR across zones or regions will have financial implications. This helps customers who must comply with governmental regulations about data retention where it is generated (Canada and Germany both have regulations requiring local data storage within the country, for example).

BCP Considerations

Business continuity practices vary greatly from organization to organization. Some companies view the tasks associated with backing up data as application-specific – and they view data backup as a business unit. Prime examples include law firms and pharmaceutical firms that rely on documentation for their lawsuits, and drug certifications and patents.

An important question that merits strategic thinking is: Should companies rely on their cloud services suppliers to take care of data backup/recovery for all the workloads they support on behalf of the customer's business?

Alternatively, should the primary responsibility fall on IT organizations that have labored for years to institute best practices via data policies – and to test their DR/BC practices quarterly or annually.

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; *Contact: inquiry@rfgonline.com*

Additional considerations include: whether data supported by means of active/active backup – across multiple data centers. They should also understand whether the hybrid cloud is rapidly becoming the means by which periodic backups for on-prem and off-prem systems take place? It remains to be seen how the "mix" of DR/BC approaches will evolve in this COVID-19 New Normal environment.

Finally, thought must be given to geographic considerations, where data generated within a country or region must remain in that geography – even when it's being backed up for disaster recovery (DR) or business continuity (BC) purposes.

SUMMARY

Content delivery networks (CDNs) and CSPs offer enterprises a vast array of DR and BC options that did not exist in the pre-cloud era. Because cloud providers offer a wide range of compute, storage and networking services, business and IT executives must carefully evaluate which options are best for their organizations.

RFG POV: The WFH hybrid multi-cloud environment is much more complex than the bounded work/data center environment that existed not long ago. To succeed in the New Normal work environment, businesses must design for failure; simplify and standardize their environments; automate with AI/ML as much as possible; and communicate their vision and actions to customers, employees, business partners, and stakeholders. Given the New Normal computing environment, business and IT executives should view the WFH business environment as a marketing advantage and opportunity, rather than as a pure cost element of doing business.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, President of Cloud Architects Advisors LLC, co-authored this report.

---

46 Kent Hills Lane, Wilton, CT. 06897; (203) 429 8951;
http://www.rfgonline.com/; Contact: inquiry@rfgonline.com