



## HOW TO SETUP A HIGHLY RESPONSIVE BC/DR SOLUTION WITH NEAR-ZERO RECOVERY PERIOD AT UP TO 80% LOWER COST?

When agencies transform their IT systems to address the digital imperative, one thing that doesn't get the attention it deserves is disaster recovery (DR).

Being more digital means being more dependent on technology. This increases the risk of disruption due to cyberattacks, natural disasters or hardware/software failures. Any disruption can have significant financial and security impact, especially for public sector organizations that manage sensitive data.

The frequency and severity of these disruptions appears to be increasing. For example, in 2016 the IRS had to stop accepting electronically filed tax returns due to a hardware failure<sup>1</sup>. In 2015, a significant equipment failure at one of the data centers brought down a number of federal government websites in Canada<sup>2</sup>. And more recently, an error brought down US State Department's email service for half-a-day<sup>3</sup>.

These outages impact workers' ability to do their job, they impact constituents, and they are extremely expensive - the average cost of downtime can range from \$5600 per minute<sup>4</sup> to \$8000 per minute<sup>5</sup>. This can be prohibitive for public sector organizations, especially if they take days<sup>6</sup> to recover from a disruption.

To minimize the cost and the broader impact of a disruption, public sector organizations need to keep their business continuity plans updated. A highly responsive disaster recovery solution with sub-second Recovery Period Objective (RPO) and Recovery Time Objective (RTO) is a critical component of this plan. Meeting these requirements through traditional DR models can be expensive.

## Common DR approaches: Balancing cost and recovery period

Typically, public sector organizations use either of these two approaches for their disaster recovery solution:

1. Physical or Off-site
2. Backup based as-a-service

The physical or off-site DR approach can offer very short RPO and RTO (Hot DR), but also requires extensive investments in hardware (duplicate servers), software licenses, DR infrastructure and services (data protection software, replication software, high-speed connectivity etc.), and management (IT staff for maintenance & support of the DR systems).

**A large enterprise (with more than 750 servers) may spend an average of \$11 Mn/year to setup and maintain a physical DR site. This is a significant amount of money, especially for budget constrained public sector organizations<sup>7</sup>.**

Disaster Recovery As-a-Service (DRaaS) offers a cheaper alternative. With DRaaS, organizations leverage a third party vendor to provide DR infrastructure and services. The third-party hosts physical or virtual servers, generally on a cloud, for an organization. DRaaS uses a backup or snapshot-based approach to sync data between production and recovery sites. The third-party manages the hardware and software, services and monitors the DR solution and is responsible for providing failover according to the defined service level agreements.

**With DRaaS, a large enterprise may spend less on its DR setup as compared to the physical or off-site model. However, if the DRaaS setup uses a snapshot based replication technology, then the organization is unlikely to realize sub-second RPO & RTO<sup>7</sup>.**

The other challenge with these two options is the testing of the DR setup. Ideally, a DR system should be tested every six months. This requires planning and provisioning of resources, including staff time which is already in short supply. Testing a physical DR setup or a DRaaS setup can take days and a lot of commitment from many people.

## Re-thinking DR to realize near-zero RPO at a cost savings of up to 80%

Organizations spend a lot of effort and money in maintaining the DR setup – facility costs, maintenance of duplicate resources (hardware and software licenses), manpower etc.

Cloud-based DR that uses block-level continuous data-replication and helps an agency provision the resources when needed instead of all the time can not only help achieve sub-second RPO but also lower cost by up to 80%.

## Cloud can help do more at a lower cost

The cost of cloud storage is less than conventional storages. For example, cost of storage on AWS' most optimized storage could be as little as \$4000 a month for 1 Peta Byte of storage (see the table below).

Storage	\$/GB	10 TB	1 PB
Standard	\$0.0230	\$230	\$23,000
Infrequent Access	\$0.0125	\$125	\$12,500
Glacier	\$0.0040	\$40	<b>\$4,000</b>

Other leading cloud providers like Microsoft Azure and Google are priced similarly.

DR setup is far more scalable with a cloud solution. Organizations can increase or decrease capacity based on their need, without investing a lot of effort.

## Block-level replication for sub-second RPO

Back-up or snapshot based approaches sync-up data in distinct intervals. This means no near-zero RPO and significant expense (in terms of data transfer costs). Real-time replication can deliver sub-second RPO and optimize data transfer cost, but can also impact performance of existing systems.

Continuous block-level replication technologies offer a effective alternative, providing a highly responsive DR solution at a fraction of the cost. This approach captures changes (including but not limited to files, file system changes, RAID configurations, databases, OS configuration etc.) in real-time and replicates only those changes to the target location in an asynchronous manner. Not only does this minimize the impact on the performance of existing operations but this approach also delivers sub-second RPO in case of failover.

Organizations can further reduce cost

of their DR setup by replicating data in a staging area, instead of the target environment, and using automated tools to quickly clone the data from the staging area to the target environment in case of a disaster.

With this approach, organizations:

- Don't have to maintain or pay for duplicate provisioning of resources (servers, software licenses.) Instead, they just need to pay for a light-weight "replication staging area" to keep their data and apps in sync during normal operations
- Automate sync up of servers, apps etc. and minimize the resources need to manage or monitor the DR solution

Not only is this option cheaper – a large enterprise may have to spend as little as

\$650K to setup its DR systems<sup>7</sup> – but also offers a number of benefits including:

- Self-service configuration of cloud environment, replication of servers etc.
- Sub-second RPO and RTO in minutes
- Easy and cost-effective testing
- Flexibility to move between cloud providers and even automatically convert machines from one infrastructure to another

## A comparison of the three DR strategies<sup>7</sup>

	On-Premise	As-a-Service	Cloud-based
Total cost of ownership	High	Medium	Low
Cost & effort on deployment and maintenance	High	Medium	Low
Simplifies and supports quick testing?	No	No	Yes
Scalability	Low	Medium	High

### How to choose the right cloud-based DR solution?

There are multiple cloud-based DR solutions. Some may not support all the applications or work with any cloud provider, some may impact server performance, and some may not deliver the required RTO or RPO. Block-level replication and a low-cost staging area are just a couple of factors that organizations should consider while selecting a cloud-based DR solution. Some others include:

- 1. Automated conversion of servers to any infrastructure** – As cloud technology evolves, organizations may need to convert their servers from the old infrastructure to the cloud of their choice. A solution that offers automated conversion would score over any other solution since it will make it easier for organizations to switch between infrastructures and keep their solution current without spending too much time and effort
- 2. Robust security** – Since data and information are being replicated,

the solution should encrypt the data using the most powerful models and should also support data transmission through private networks like an organization's own VPN

- 3. On-demand testing** – DR testing is important. The solution should offer options to conduct tests quickly, cost-effectively, and without extensive planning or preparation

### Conclusion

The digital imperative and the increasing frequency and severity of attacks –physical, cyber, and human - are making disaster recovery more crucial than ever. Public sector organizations need to ensure that their disaster recovery solution can help them recover within seconds. Doing this with traditional approaches (on-premise, DRaaS) can be costly. Moving DR to the cloud provides public sector organizations with the opportunity to implement a highly secure, enterprise-grade disaster recovery solution at a savings of up to 80%.

## References

1. "IRS Website Hit With Hardware Failure, Some Refund & Payment Tools Unavailable," Forbes, <https://www.forbes.com/sites/kellyphillipserb/2016/02/03/irs-website-hit-with-hardware-failure-some-refund-payment-tools-unavailable/#dbae9212476a>
2. "Computer outage shut down key government websites, email for hours," Ottawa Citizen, <http://ottawacitizen.com/news/local-news/computer-outage-shuts-down-key-government-websites-email>
3. "U.S. State Department email restored after global outage," Reuters, <https://www.reuters.com/article/us-usa-statedepartment-email/u-s-state-department-email-restored-after-global-outage-idUSKCN1AY1QO>
4. "The Cost of Downtime," Gartner, <https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>
5. "Study: Data Center Downtime Costs \$7,900 Per Minute," DataCenter Knowledge, <http://www.datacenterknowledge.com/archives/2013/12/03/study-cost-data-center-downtime-rising>
6. "Survey Says: Government IT System Outages are Painful, Not Uncommon," Center for Digital Government, [http://infotech.report/Resources/Whitepapers/673b2129-90af-4e80-aac6-8830090915c3\\_Survey%20Says%20Government%20IT%20System%20Outages%20Are%20Painful%20and%20Common.pdf](http://infotech.report/Resources/Whitepapers/673b2129-90af-4e80-aac6-8830090915c3_Survey%20Says%20Government%20IT%20System%20Outages%20Are%20Painful%20and%20Common.pdf)
7. "Finally, Affordable Enterprise-Grade Disaster Recovery Using the Cloud," CloudEndure, <https://info.cloudendure.com/rs/094-DCS-290/images/2016%20How%20Cloud%20DR%20Reduces%20Costs%20-%20WP.pdf>

For more information, contact [askus@infosyspublicservices.com](mailto:askus@infosyspublicservices.com)



---

© 2018 Infosys Public Services, Inc., Rockville, Maryland, USA. All Rights Reserved. Infosys Public Services believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys Public Services acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Public Services and/ or any named intellectual property rights holders under this document.

[Infosyspublicservices.com](http://Infosyspublicservices.com)

Stay Connected  