CenturyLink® Business

WHITE PAPER

Minimize IT Downtime with DRaaS

WHITE PAPER

Minimize IT downtime with DRaaS: Cloud Technology Delivers Value for DR Workloads

How long can your business systems be out of commission? A day? An hour? A minute? In today's dynamic (and demanding) business environment, every moment counts, which means the tolerance-for-downtime is getting smaller and smaller. Unfortunately, the risks that can take your business down — hard — are getting bigger and bigger.

Many CIOs want to keep disaster recovery (DR) systems running in-house. A key part of their DR strategy is determining whether the ability to recover is more effectively handled on premise or in an outsourced hosting environment. The preponderance of catastrophic IT failures often stems from employee/administrator error, natural disasters or cyber security events such as Distributed Denial of Service (DDoS) attacks. Meanwhile, protecting core systems can be complex and expensive. Many organizations are not equipped to provide the requisite remote data centers, special expertise, and recovery software/hardware systems. Increasingly, executives are turning to managed services or cloud infrastructure as a cost-effective and reliable option for disaster recovery protection.

No wonder 66% of Forrester survey respondents report DR to be a high or critical business priority (Source: Forrester 2013). It is expected that many will continue to use on-site or traditional hosted DR services while others will take advantage of cloud-based DRaaS (Disaster Recovery-as-a-Service) within the next five years. In fact, sales of cloud-based DR services are expected to increase by 23% by 2016. The opportunity is real and it's growing. New cloud capabilities allow businesses to deploy a cost efficient solution, removing the need to provision a remote site, have physical and virtual infrastructure there and ensure dedicated high-speed data links are in place, as well as a redundant operating system and application licenses.

Even the biggest and most tech-savvy of companies is not immune. On Jan. 27, Facebook services were down not for just a few minutes — which in itself would have been big news —but for a full hour.

Although a hacking group took credit for causing the outage, which also affected the Instagram service, Facebook issued a statement saying that the issue was caused by a change the company implemented that affected its configuration systems. "We moved quickly to fix the problem, and both services are back to 100% for everyone," according to the statement.

Some would argue that an hour isn't very quick, especially when you think about the number of people — and businesses — whose continuity depends on Facebook. And while the outage apparently wasn't caused by a hacking group, that scenario is totally plausible given the increase in hacks (and in the sophistication of those hacks) we have been seeing — on companies as big as Facebook but on small and midsize companies, as well. Further, the actual cause of the outage, according to Facebook — a configuration change — is something every company does on a regular basis.

Indeed, the downtime dilemma crosses company size, industry and region.

A December 2013 Ponemon report found that 91 percent of data centers had experienced unplanned downtime in a 24-month timespan. And companies paid a high price for that downtime: Complete or partial unplanned data center outages in a 12-month period in 67 data centers across the United States totaled a collective loss of more than $46 million, according to the Ponemon report.

"Industries with revenue models dependent on the data center's ability to deliver IT and networking services to customers — such as telecommunications service providers and ecommerce companies — and those that deal with a large amount of secure data — such as defense contractors and financial institutions — continue to incur the most significant costs associated with downtime," stated the report.

Preparing for the Worst

A company's ability to resume business after a cyberhit is directly tied to its ability to compete in today's dynamic and demanding business environment.

There are many different ways to look at disaster recovery, but, at its core, it's pretty simple, said Scott Good, Product and Solutions Marketing at CenturyLink. "Disaster recovery is the ability to get your business back up and running after a calamity. Period," he said. "Revenue or brand protection, application protection, basic data replication — that's what we're talking about here: Is it an immediate thing that's affecting the company's revenue and reputation or brand? A fix has to happen — right away."

"Disaster recovery is the ability to get your business back up and running after a calamity. Period."

Scott Good Product and Solutions Marketing, CenturyLink

The first step is to accept that disasters happen and that they are happening more frequently. Not just of the technology kind, we have witnessed floods, fire, hurricanes, tornadoes, tsunamis, blizzards ... Mother Nature certainly contributes her share to the disasters that can interrupt business operations.

Then there's the human factor: People, whether through malice aforethought or simple error, are among businesses' biggest risks.

At this point in the report, you may be thinking to yourself, "No problem — I have a disaster recovery system in place. If my systems get taken down, I can get the business back up and running in no time." But can you? To determine your disaster recovery readiness, check to see if you can you answer "yes" to the following questions.

- Are all of your data and systems replicated? Offsite?
- If systems at your primary site did go down — or go completely dark — can you count on the network between the primary site and the secondary site? Do you know who owns that network?
- Has the disaster recovery plan been tested? How often?
- If the plan is for an individual business unit, has that plan been tested for integration with the company's general DR plan?
- Is the technology specified in the plan still in use at the company?
- Are the people/job roles specified in the plan still with the company?

Many commonly believe they can effectively recover from a disaster, but they don't actually have the people, processes and products in place to deal with today's complicated threat landscape, customer expectation for 24/7 uptime, and increasing data volumes. And many don't consider all the elements of disaster recovery planning — communications, readiness, testing, understanding, training and ability — when assessing their own DR competency.

The Disaster Recovery Preparedness Council noted in its State of Global Disaster Recovery Preparedness Annual Report 2014 that more than 60% of those who took the survey do not have a fully documented DR plan, while 40% said their DR plan was not very useful when it had to be put into place. Further, the report states, one-third of organizations participating in the survey test their DR plans only once or twice a year, and 23% never test their DR plans at all. Alarmingly, the report also found that 65% of companies that do test their plans don't pass their own tests.

Making the DR Difference

The problems are all too real, and the solutions can be overwhelming, expensive, difficult to manage, and, as the Disaster Recovery Preparedness Council found in its research, ultimately ineffective.

The good news is that the cloud provides new recovery opportunities for businesses. Cloud-based DR solutions allow businesses to deploy a cost efficient solution, removing the need to provision a remote site, have physical and virtual infrastructure there and ensure dedicated high-speed data links are in place, as well as a redundant operating system and application licenses. In short, Cloud infrastructure coupled with Disaster Recovery Management software make business continuity more accessible for agencies and often delivers traditional value at much lower prices.

New Disaster Recovery-as-a-Service (DRaaS) solutions are augmenting the power of the cloud, enabling businesses to run hybrid production IT systems in their multiple data centers during normal operations, and to spin up exact replica data centers as the need arises. Most importantly, DRaaS can help businesses attain and maintain the kind of agility and resilience that is critical in today's ever- and quickly changing world.

There are many advantages to Disaster Recovery-as-a-Service, including:

- The ability to move disaster recovery activities and infrastructure from capex to opex.
- The ability to adopt a flexible, pay-as-you-go model
- The ability to quickly and easily scale DR protection as business needs (or outside security influences) dictate
- Regular testing to ensure that the DR plan in place meets immediate organizational needs
- Access to DR expertise and services, allowing businesses to focus on their core competencies

A recent report by research firm TechNavio noted that the DRaaS market is expected to grow at a CAGR of more than 50% through 2019. "Adoption of hybrid cloud disaster recovery services by businesses eliminates the need for a secondary disaster recovery site, enhances traditional disaster recovery solutions and delivers disaster recovery solutions for remote offices," according to a BusinessWire story on the report. "Hybrid cloud DRaaS will also help reduce expenses, retain data on premises for fast local recovery and protect physical and virtual operating systems and applications."

As companies in all industries work to balance today's 24/7 business demands with increasing (and increasingly dangerous) security threats, the cloud and Disaster Recovery-as-a-Service are providing real, tenable platforms that enable organizations to effectively plan for the worst while they focus on being the best.

"Hybrid cloud DRaaS will also help reduce expenses, retain data on premises for fast local recovery and protect physical and virtual operating systems and applications."

BusinessWire

Government Callout

America's top soldier, Gen. Martin E. Dempsey, chairman of the Joint Chiefs of Staff, is concerned. While he has every confidence in the U.S.' military prowess, he recognizes there is a new battlefield where cybersecurity threats continue to grow. "In every domain, … we generally enjoy a significant military advantage. But we have peer competitors in cyber," Dempsey said on Fox News Sunday.

"We don't have an advantage. It's a level playing field. And that makes this chairman very uncomfortable."

Our government systems are vulnerable, as evidenced by the recent hijacking of the Twitter and YouTube accounts of U.S. Central Command. The hack was purportedly committed by actors supportive of the terrorist group Islamic State, also known as ISIS. Coincidentally (or perhaps planned), the hack took place just as President Obama was addressing the Federal Trade Commission on the subject of … cybersecurity.

It can be argued that business continuity is more critical in some industries than in others — but few more so than government.

In fact, government data centers have had their share of the spotlight lately. In 2010, the Federal Data Center Consolidation Initiative (FDCCI) was created to reverse the historic growth of federal data centers. This program has achieved great cost savings, according to the Government Accounting Office, but other metrics must be considered, as well. A 2014 survey conducted by public-private IT partnership MeriTalk found that many government workers have little confidence in the resilience of their respective agencies' data centers.

Meritalk surveyed 300 federal IT workers who either worked in data centers or were responsible for data center policy or functions. Thirty-six percent of those surveyed don't think their agency is going a good job of managing downtime at their data centers. Perhaps more concerning, 29 percent said they don't think their agency fully understands the impact of downtime on the organization. Respondents said they thought their agencies lacked the computational power, personnel and data storage needed to provide a reliable data center.

Fortunately, government agencies have also been given a cloud-first directive: "To harness the benefits of cloud computing, we have instituted a Cloud First policy. This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."

When it comes to disaster recovery, the cloud — augmented by Disaster Recovery-as-a-Service (DRaaS) — is enabling government agencies to attain the kind of "level playing field" that Gen. Dempsey referenced.

DRaaS offers government agencies the ability to cut costs with a flexible, pay-as-you-go model, to effectively scale DR protection as needs dictate, to test regularly to ensure that the DR plan in place meets existing needs and mandates, and to access cybersecurity and disaster recovery expertise, allowing government agencies, workers and even Gen. Dempsey to focus on the country's — and its citizens' — most pressing concerns.

About CenturyLink Cloud

CenturyLink Cloud is the complete platform to easily manage your entire business application portfolio, from development to business-critical workloads. CenturyLink Cloud offers high-performance, scalable, self-service virtual machines across our global network of data centers, including Hyperscale instances for distributed workloads that require maximum performance. And CenturyLink Cloud provides built-in automation, orchestration, and management tools for an IT-ready and developer-friendly platform that is flexible, scalable, cost effective and highly manageable.

For more information, visit
www.centurylinkcloud.com/disaster-recovery

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

Global Headquarters
Monroe, LA
(800) 728-8471

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6591 8824

Canada Headquarters
Toronto, ON
1-877-387-3764

CenturyLink® Business