CARBONITE

How to disaster-proof critical business data

5 steps for keeping systems online and accessible in any scenario.

The growth of DRaaS

The tremendous growth of software as a service (SaaS) continues, while businesses continue to benefit from the many administrative, organizational and economic advantages offered by this model. The disaster recovery industry is no exception.

Gartner estimates the global disaster recovery as a service (DRaaS) market at approximately $1.7 billion currently, with a compound annual growth rate of around 25 percent. Within the next year or so, Gartner predicts the DRaaS market will surpass more traditional subscription-based DRaaS.[1]

Relative to their size, smaller businesses stand to benefit the most from the move to DRaaS, because they're least able to absorb extra administrative costs—in terms of both time and budget. Remove those costs and the benefits are immediately impactful.

In a recent report, Gartner credited improved functionality and affordability for the skyrocketing growth of DRaaS among small and midsize businesses. In other words, the industry has actualized the improvements these customers needed to see before they could make the switch.

As a result, Gartner estimates the DRaaS market will nearly triple rising to $3.4 billion by 2019. Larger companies are making the switch as well, for the same reasons. Gartner reported a 77 percent increase in inquiries from enterprises in 2015. In this case, where they go, smaller organizations would be wise to follow.[1]

[1] http://www.storagenewsletter.com/rubriques/market-reportsresearch/magicquadrant-for-disaster-recovery-as-a-service-gartner-2/

How to disaster-proof critical business data

5 steps for keeping systems online and accessible in any scenario.

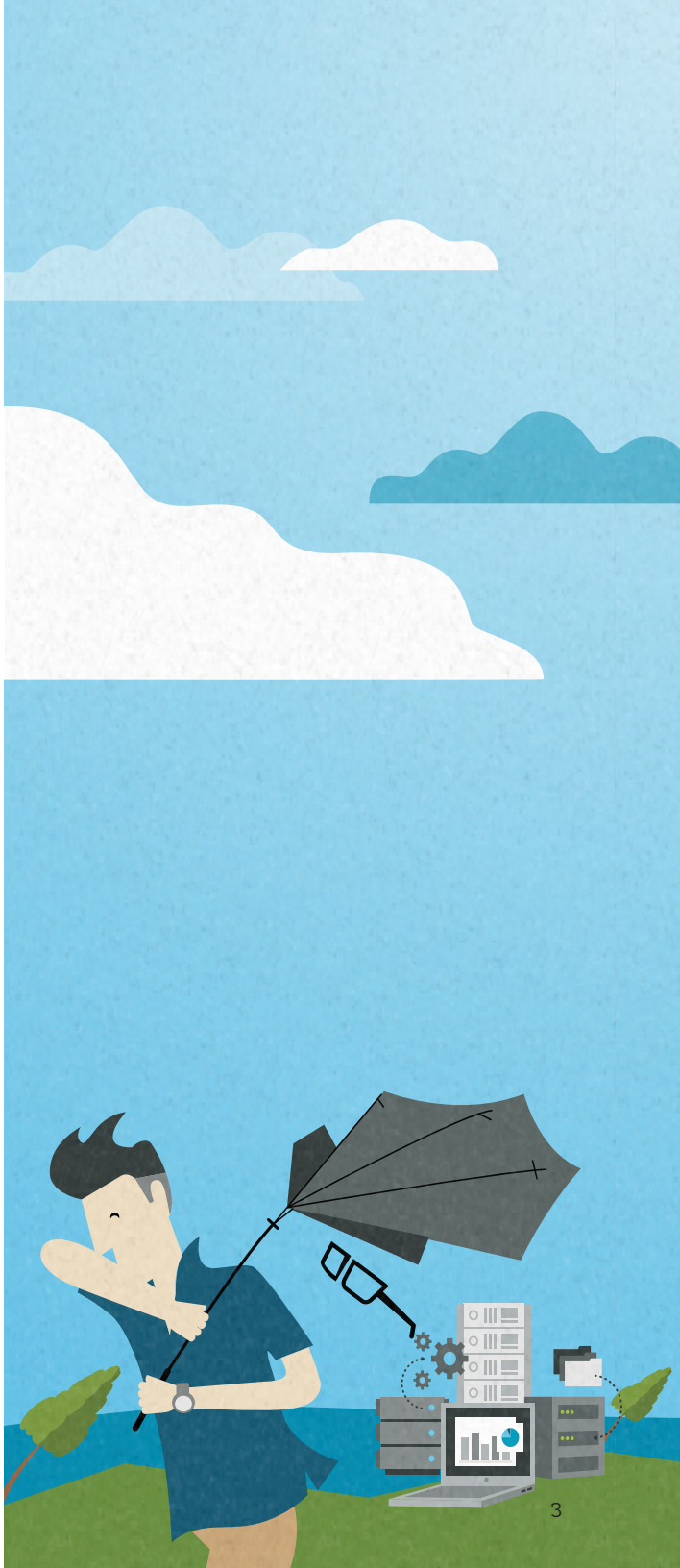
Downtime costs drive the need for protection

Big guys can take an occasional hit—but smaller guys can't afford the loss

The tangible costs of a downtime are real, and for some, they're devastating. A recent survey of IT professionals produced some sobering expectations.

Two-thirds (67 percent) say their business losses would exceed $20,000. On the higher end of the scale, 27 percent say that downtime would cost more than $100,000 per event.[2] Those figures consider only the measurable losses, though employee productivity would take a huge hit, along with the delivery of products and services, and damage to the reputation of the company.

A customer lost, whatever the reason, is a customer that's likely lost forever. When disaster strikes, it's always unexpected. The businesses that survive are the ones that are best able to weather the storms. And that's why disaster recovery should be top of mind for any business. It's simply not a case where "better late than never" applies.



[2] http://www.marketwired.com/press-release/zetta-state-disaster-recovery-survey-reveals-90-it-professionals-using-cloud-their-dr-2176272.htm

How to disaster-proof critical business data

5 steps for keeping systems online and accessible in any scenario.

Why it matters to have a plan in place

Lost revenue during downtime

Even short downtime events can be damaging. Fifty-three percent of organizations surveyed can tolerate less than an hour of downtime before they begin to experience significant revenue loss.[3]

It all eventually adds up—over a five-year period, businesses lost over $70 million due to downtime alone.[4] And downtime revenue loss is really just the tip of the iceberg.

Lost productivity

IT professionals talk a lot about the hidden costs of disasters. When disaster strikes and data is unavailable, there's no chance to add revenue, of course, but in a broader sense, there's little to no chance to do much else. When the data is gone, it's gone for everyone.

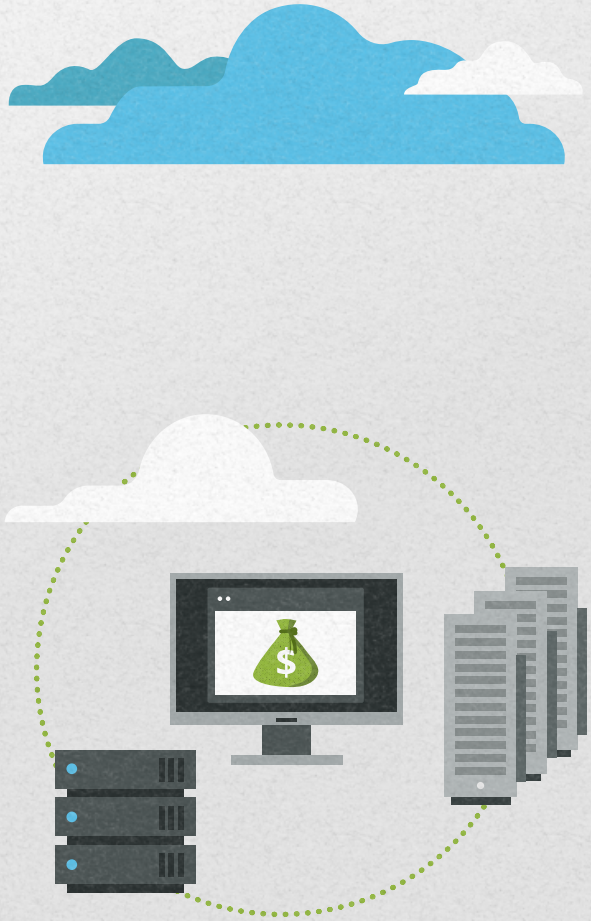
Loss of customer trust

Loss of customer faith is a particular problem in the case of data breaches, but it can also apply more generally to failures to deliver as expected. Trust is earned over time, and once it's lost, it's nearly impossible for a business to regain it—especially in an age of seemingly limitless choices for customers.

Business failure

Business failure is not just a threat; it's the most likely result when you're not prepared for the worst. The numbers bear this out: 75 percent of companies without a business continuity plan go out of business within three years of a disaster.[5]

You can avoid adding to that total—if you follow these five steps to building an effective disaster recovery strategy. Remember, there's no telling what's around the corner, so the best way forward is to make sure you're ready for anything.



[3] http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/T/The-Importance-of-a-Disaster-Recovery-Plan.aspx

[4] https://www.rockdovesolutions.com/blog/risk-costs-of-not-having-a-business-continuity-management-program.

[5] http://www.washsq.com/home/newsletter/the-normalcy-bias-an-obstacle-to-effective-disaster-recovery-business-continuity-preparations

The five steps

1. Identify

2. Assess

3. Customize

4. Blend

5. Repeat

How to disaster-proof critical business data

5 steps for keeping systems online and accessible in any scenario.

Step 1: Identify

IT assets: Inventory and map all of your IT assets, listing dependencies as you go.

Important business processes: Identify which IT-related business processes are critical to staying operational, as you'll need to consider those first when forming your strategy.

Zero downtime is typically required for these mission-critical or "Tier 1" systems and applications. The level of protection you deploy for Tier 1 data can be higher than for less critical data. This layered approach ensures high levels of uptime, or high availability, for critical data while managing total cost of ownership (TCO).

The answers you come up with in the first step will depend on the type of business. For a healthcare practice, critical data includes electronic medical records (EMR) and protected health information (PHI). For a company that depends on its website for revenue, keeping the website up and running will likely be the top priority. Any data that is essential for the continued flow of critical business operations should be considered Tier 1 data. In addition, any data that's protected by a regulatory framework is considered critical data, and protection may be stipulated for compliance, licensing and accreditation. These assets typically require more stringent recovery time and recovery point objectives (RTO/RPO).

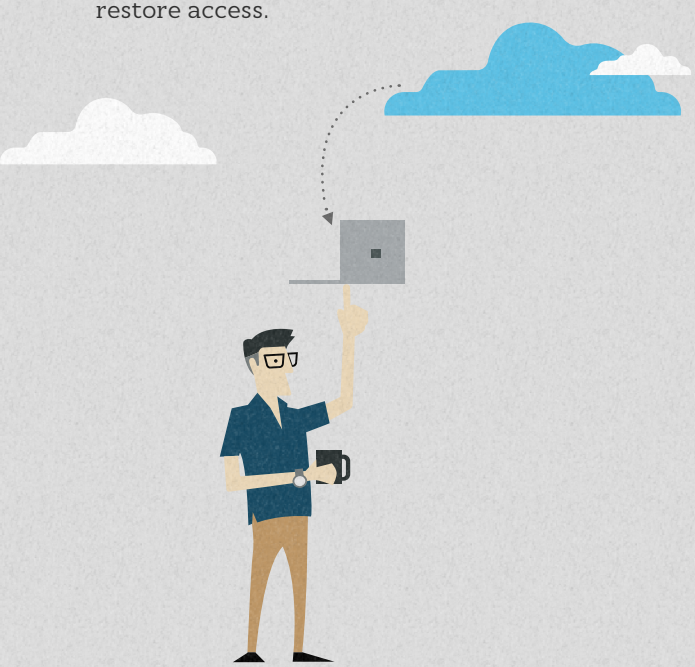
In Other Words...

To determine RPOs, answer this question: "Up to what point in time does the business process need to be restored in order to effectively resume operations?"

Think of RPO as the interval of time between the last backup and the disaster event.

To determine RTOs, answer this question: "What is the acceptable amount of time it can take to restore each process to the desired RPO?"

Think of RTO as the interval of time between the disaster event and when you successfully restore access.



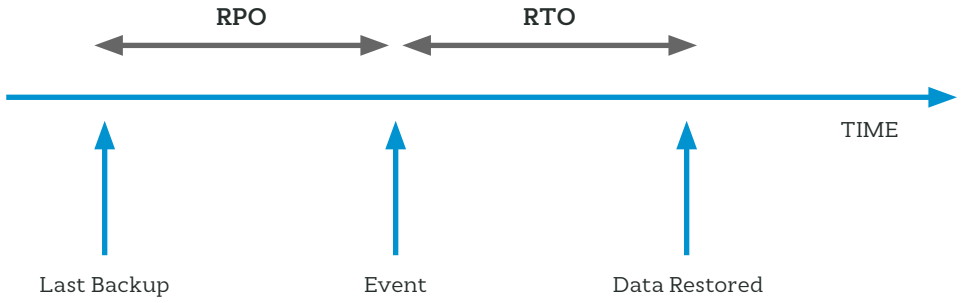
Step 2: Assess

Business impact: After identifying the IT business processes in step one (e.g., email or billing systems), assign each one to a tier. Tier 1 includes the mission-critical applications, systems and regulated data you identified in step one. The processes in Tier 2 would be of mid-level importance, and Tier 3 would follow, with the lowest priorities.

Next, label the items in each tier with the appropriate recovery point objective (RPO) and recovery time objective (RTO). See the sidebar for simple explanations you can use to help get those less technical up to speed.

Downtime costs: Estimate the real cost of downtime for each of your processes and systems. Determine how much it would cost for these systems to be offline. This includes direct costs like lost transactions and revenue, and the cost of remediation. It also includes indirect costs like damage to brand reputation and customer loyalty. This will help you prioritize and get buy-in on a disaster recovery solution from decision-makers. Breaking down your technology assets based on this framework helps ensure you're deploying resources where you most need them.

Identify internal SLAs as well as customer/supplier SLAs, and document the costs of not meeting those agreements. Or, if your ERP system were down, how much would that cost in 15-minute intervals?



Step 3: Customize

Decide the order in which certain business operations will be restored in the event of an interruption—based on dependencies, tiers and RPOs/RTOs.

For a revenue-generating website, "restore" might be a misnomer. Protection for always-on systems is not measured by recovery time but rather by percentage of system uptime. This level of service extends protection beyond the practice of disaster recovery and into the realm of high availability (HA).

Once you've classified assets based on tiers, you can customize protection based on the objectives you established in the previous step.

The goal is a defined plan based on business requirements that ensures continuity of critical systems if disaster strikes. This means everything should be inventoried and mapped—gather floor plans, utility diagrams, system configurations and every other relevant bit of information.

Your customized disaster recovery plan should consider the likelihood of various threats and how the response might be different for each. An accidental deletion, for example, will require a different recovery procedure than a flood or a fire. Procedures should be laid out, as well as responsibilities for each stakeholder.

Consider developing response teams, and then determining the level of training required for each team member, so that everyone is prepared for whatever may come.

However your plan is customized, make sure you test it thoroughly. You don't want to wait until after a disaster to discover your plan is missing a critical piece.

Step 4: Blend

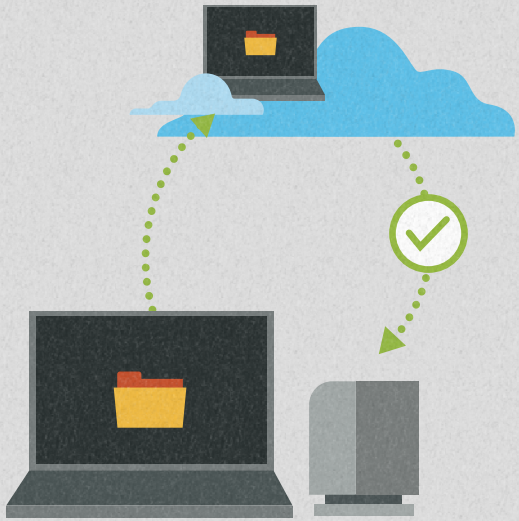
Supplement cloud backup with on-premises protection and high availability for critical workloads. There's no such thing as a one-size-fits-all approach. Your organization's needs are unique, so it's more than likely you'd be best served by a blended plan. Carbonite offers a complete platform of high availability, backup and disaster recovery solutions that can satisfy this approach.

Secure cloud backup is a must, because your data is kept safe offsite, far from whatever physical disaster may occur onsite. But onsite protection can offer faster recovery capability in cases where the disruption is contained to local failure, accidental deletion or file overwrite. And instant failover, an option for high availability deployments, can help businesses achieve near 100 percent uptime service levels for those systems that need it.

Critical workloads and databases built up over years must be kept safe and retrievable, and a blended approach is the best bet for a full recovery.

Step 6: A Flexible Vendor

We confess: We snuck an extra step into the list. But finding a partner you can trust, with flexible pricing and configurations (hardware as a service, on premises, cloud and high availability) is where the rest of the steps all come together. For obvious reasons, an easy user experience is essential for simple administration, along with security and compliance considerations. Carbonite can help you develop and execute a customized disaster recovery strategy that pays off when it matters most. And for a business, that can mean the difference between surviving a catastrophic disaster and going out of business.



Step 5: Repeat

Testing is a critical part of your disaster recovery strategy. For some businesses, testing and reporting are both mandated by regulations. A recent survey of IT pros found that only 40 percent of companies test their DR plans annually. Another 28 percent test their plans only rarely, if ever.[6]

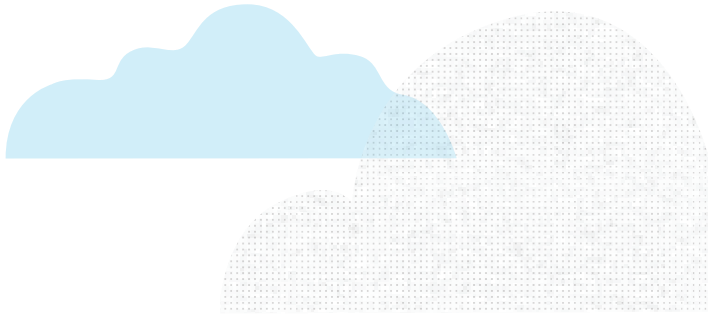
As businesses and technology evolve over time, so will protection needs. Your disaster recovery strategy is only useful if it's updated regularly to keep up with changes. Flexible technology that adapts to innovations while still supporting legacy systems is essential for long-term security.

[6] http://www.marketwired.com/press-release/zetta-state-disaster-recoverysurvey-reveals-90-it-professionals-using-cloud-their-dr-2176272.htm

How to disaster-proof critical business data

5 steps for keeping systems online and accessible in any scenario.

Carbonite's complete data protection platform offers businesses every level of protection they need for their entire infrastructure. To discuss our dependable DRaaS and high availability (HA) offerings, including please call **800-683-4667** or email DataProtectionSales@carbonite.com.



CARBONITE™